(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3792896号
(P3792896)
(45)発行日　平成18年7月5日(2006.7.5)　(24)登録日　平成18年4月14日(2006.4.14)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	520F
G11B 20/10	(2006.01)	G06F	12/14	540B
G06F 21/22	(2006.01)	G11B	20/10	H
		G06F	9/06	660E

請求項の数 7　(全 149 頁)

(21)出願番号　特願平10-161660
(22)出願日　平成10年5月13日(1998.5.13)
(65)公開番号　特開平11-283327
(43)公開日　平成11年10月15日(1999.10.15)
審査請求日　平成17年5月10日(2005.5.10)
(31)優先権主張番号　特願平9-122511
(32)優先日　平成9年5月13日(1997.5.13)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願平10-16618
(32)優先日　平成10年1月29日(1998.1.29)
(33)優先権主張国　日本国(JP)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100068814
弁理士　坪井　淳
(74)代理人　100092196
弁理士　橋本　良郎
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】情報再生装置及び情報再生方法

(57)【特許請求の範囲】
【請求項１】
暗号化されたコンテンツ情報を復号するための復号鍵と、前記コンテンツ情報の利用期限及び該コンテンツ情報の復号が許可された特定復号ユニットを識別するための第１のユニットＩＤを含む利用条件とを結合して、該復号鍵と該利用条件とが不可分となるように暗号化された付加情報と、前記暗号化されたコンテンツ情報とが記録された記録媒体から、前記付加情報及び前記暗号化されたコンテンツ情報を読み出す読出手段と、
前記読出手段で読み出された前記付加情報を復号する復号ユニットと、
前記復号ユニットから出力された前記復号鍵を用いて、前記読出手段で読み出された前記暗号化されたコンテンツ情報の復号・再生を行う再生手段と、
を含む情報再生装置であって、
前記復号ユニットは、
前記付加情報を復号するための鍵情報を記憶する記憶手段と、
前記鍵情報を用いて前記付加情報を復号し、前記復号鍵、前記利用期限及び前記第１のユニットＩＤを得る第１の復号手段と、
時刻を計測する時計手段と、
前記利用期限が無期限・永久使用可の場合には、当該復号ユニットがもつ当該復号ユニットを識別するための第２のユニットＩＤと前記第１のユニットＩＤとが一致したとき、前記コンテンツ情報の利用が可能と判定し、前記利用期限が無期限・永久使用可でない場合には、前記時計手段が示す現在時刻が前記利用期限以前であるとき、前記コンテンツ情

報の利用が可能と判定する判定手段と、
前記判定手段で、前記コンテンツ情報の利用が可能と判定されたとき、前記復号鍵を前記再生手段へ出力することを特徴とする情報再生装置。
【請求項２】
暗号化されたコンテンツ情報を復号するための復号鍵と、前記コンテンツ情報の利用期限、該コンテンツ情報の復号が許可された特定復号ユニットを識別するための第１のユニットＩＤ及び特定記録媒体を識別するための第１のメディアＩＤを含む利用条件とを結合して、該復号鍵と該利用条件とが不可分となるように暗号化された付加情報と、前記暗号化されたコンテンツ情報とが記録された記録媒体から、前記付加情報及び前記暗号化されたコンテンツ情報を読み出す読出手段と、
前記読出手段で読み出された前記付加情報を復号する復号ユニットと、
前記復号ユニットから出力された前記復号鍵を用いて、前記読出手段で読み出された前記暗号化されたコンテンツ情報の復号・再生を行う再生手段と、
を含む情報再生装置であって、
前記復号ユニットは、
前記記録媒体から取得された当該記録媒体を識別するための第２のメディアＩＤを得る手段と、
前記付加情報を復号するための鍵情報を記憶する記憶手段と、
前記鍵情報を用いて、前記付加情報を復号し、前記復号鍵、前記利用期限、前記第１のユニットＩＤ及び前記第１のメディアＩＤを得る第１の復号手段と、
時刻を計測する時計手段と、
前記利用期限が無期限・永久使用可の場合には、当該復号ユニットがもつ当該復号ユニットを識別するための第２のユニットＩＤと前記第１のユニットＩＤとが一致し、且つ、前記記録媒体の第２のメディアＩＤと前記第１のメディアＩＤとが一致するとき、前記コンテンツ情報の利用が可能と判定し、前記利用期限が無期限・永久使用可でない場合には、前記時計手段が示す現在時刻が前記利用期限以前であり、且つ、前記第１のメディアＩＤと前記第１のメディアＩＤとが一致するとき、前記コンテンツ情報の利用が可能と判定する判定手段と、
前記判定手段で、前記コンテンツ情報の利用が可能と判定されたとき、前記復号鍵を前記再生手段へ出力することを特徴とする情報再生装置。
【請求項３】
前記第１のユニットＩＤは、前記暗号化されたコンテンツ情報が記録された前記記録媒体から、最初に当該暗号化されたコンテンツ情報の復号・再生を行った復号ユニットのユニットＩＤであることを特徴とする請求項１または２記載の情報再生装置。
【請求項４】
前記記録媒体は、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＯＭ及びハードディスクのうちのいずれか１つであることを特徴とする請求項１または２記載の情報記録装置。
【請求項５】
暗号化されたコンテンツ情報を復号するための復号鍵と、前記コンテンツ情報の利用期限及び該コンテンツ情報の復号が許可された特定復号ユニットを識別するための第１のユニットＩＤを含む利用条件とを結合して、該復号鍵と該利用条件とが不可分となるように暗号化された付加情報と、前記暗号化されたコンテンツ情報とが記録された記録媒体から、前記付加情報及び前記暗号化されたコンテンツ情報を読み出す読出手段と、
前記付加情報を復号するための鍵情報を記憶する記憶手段と、時刻を計測する時計とを備え、前記読出手段で読み出された前記付加情報を復号する復号ユニットと、
前記復号ユニットから出力された前記復号鍵を用いて、前記読出手段で読み出された前記暗号化されたコンテンツ情報の復号・再生を行う再生手段と、
を含む情報再生装置における情報再生方法であって、
前記読出手段が、前記記録媒体から、前記付加情報及び前記暗号化されたコンテンツ情報を読み出す第１のステップと、

前記復号ユニットが、
前記鍵情報を用いて、前記第１のステップで読み出された前記付加情報を復号し、前記復号鍵、前記利用期限及び前記第１のユニットＩＤを得る第２のステップと、
前記利用期限が無期限・永久使用可の場合には、当該復号ユニットがもつ当該復号ユニットを識別するための第２のユニットＩＤと前記第１のユニットＩＤとが一致したとき、前記コンテンツ情報の利用が可能と判定し、前記利用期限が無期限・永久使用可でない場合には、前記時計手段が示す現在時刻が前記利用期限以前であるとき、前記コンテンツ情報の利用が可能と判定する第３のステップと、
前記コンテンツ情報の利用が可能と判定されたとき、前記復号鍵を前記再生手段へ出力する第４のステップと、
前記再生手段が、前記第４のステップで復号ユニットから出力された前記復号鍵を用いて、前記第１のステップで前記読出手段で読み出された前記暗号化されたコンテンツ情報の復号・再生を行う第５のステップと、
を有する情報再生方法。

【請求項６】
暗号化されたコンテンツ情報を復号するための復号鍵と、前記コンテンツ情報の利用期限、該コンテンツ情報の復号が許可された特定復号ユニットを識別するための第１のユニットＩＤ及び特定記録媒体を識別するための第１のメディアＩＤを含む利用条件とを結合して、該復号鍵と該利用条件とが不可分となるように暗号化された付加情報と、前記暗号化されたコンテンツ情報とが記録された記録媒体から、前記付加情報及び前記暗号化されたコンテンツ情報を読み出す読出手段と、
前記付加情報を復号するための鍵情報を記憶する記憶手段と、時刻を計測する時計とを備え、前記読出手段で読み出された前記付加情報を復号する復号ユニットと、
前記復号ユニットから出力された前記復号鍵を用いて、前記読出手段で読み出された前記暗号化されたコンテンツ情報の復号・再生を行う再生手段と、
を含む情報再生装置における情報再生方法であって、
前記読出手段が、前記記録媒体から、前記付加情報及び前記暗号化されたコンテンツ情報を読み出す第１のステップと、
前記復号ユニットが、
前記記録媒体から取得された当該記録媒体を識別するための第２のメディアＩＤを得る第２のステップと、
前記鍵情報を用いて、前記付加情報を復号し、前記復号鍵、前記利用期限、前記第１のユニットＩＤ及び前記第１のメディアＩＤを得る第３のステップと、　前記利用期限が無期限・永久使用可の場合には、当該復号ユニットがもつ当該復号ユニットを識別するための第２のユニットＩＤと前記第１のユニットＩＤとが一致し、且つ、前記記録媒体の第２のメディアＩＤと前記第１のメディアＩＤと一致するとき、前記コンテンツ情報の利用が可能と判定し、前記利用期限が無期限・永久使用可でない場合には、前記時計手段が示す現在時刻が前記利用期限以前であり、且つ、前記第１のメディアＩＤと前記第１のメディアＩＤと一致するとき、前記コンテンツ情報の利用が可能と判定する第４のステップと、
前記コンテンツ情報の利用が可能と判定されたとき、前記復号鍵を前記再生手段へ出力する第５のステップと、
前記再生手段が、前記第５のステップで復号ユニットから出力された前記復号鍵を用いて、前記第１のステップで前記読出手段で読み出された前記暗号化されたコンテンツ情報の復号・再生を行う第６のステップと、
を有する情報再生方法。

【請求項７】
暗号化されたコンテンツ情報を復号するための復号鍵と、少なくとも前記コンテンツ情報の利用期限を含む利用条件とを結合して、該復号鍵と該利用条件とが不可分となるように暗号化された付加情報と、前記暗号化されたコンテンツ情報とが記録された記録媒体か

ら、前記付加情報及び前記暗号化されたコンテンツ情報を読み出す読出手段と、
前記付加情報を復号するための鍵情報を記憶する記憶手段と、時刻を計測する時計とを備え、前記読出手段で読み出された前記付加情報を復号する復号ユニットと、
前記復号ユニットから出力された前記復号鍵を用いて、前記読出手段で読み出された前記暗号化されたコンテンツ情報の復号・再生を行う再生手段と、
前記付加情報を更新する更新手段と、
を含む情報再生装置における情報再生方法であって、
前記読出手段が、前記記録媒体から、前記付加情報及び前記暗号化されたコンテンツ情報を読み出す第１のステップと、
前記復号ユニットが、
前記鍵情報を用いて、前記第１のステップで読み出された前記付加情報を復号し、前記復号鍵、前記利用条件を得る第２のステップと、
前記利用条件に含まれている前記利用期限が無期限・永久使用可の場合、該利用条件に、該コンテンツ情報の復号が許可された特定復号ユニットを識別するための第１のユニットＩＤが含まれているとき、当該第１のユニットＩＤと、当該復号ユニットがもつ当該復号ユニットを識別するための第２のユニットＩＤとが一致したとき、前記コンテンツ情報の利用が可能と判定し、前記利用期限が無期限・永久使用可でない場合には、前記時計手段が示す現在時刻が前記利用期限以前であるとき、前記コンテンツ情報の利用が可能と判定する第３のステップと、
前記利用条件に含まれている前記利用期限が無期限・永久使用可の場合、該利用条件に、前記第１のユニットＩＤが含まれていないとき、前記付加情報と、当該復号ユニットの第２のユニットＩＤを前記更新手段へ出力する第４のステップと、
前記コンテンツ情報の利用が可能と判定されたとき、前記復号鍵を前記再生手段へ出力する第５のステップと、
前記再生手段が、前記第５のステップで復号ユニットから出力された前記復号鍵を用いて、前記第１のステップで前記読出手段で読み出された前記暗号化されたコンテンツ情報の復号・再生を行う第６のステップと、
前記更新手段が、前記第４のステップで前記復号ユニットから出力された付加情報に含まれる前記利用条件に、前記第４のステップで前記復号ユニットから出力された前記第２のユニットＩＤが追加された新たな付加情報を生成する第８のステップと、
前記更新ユニットが、前記新たな付加情報で前記記録媒体に記録されている前記付加情報を書き換える第９のステップと、
を有する情報再生方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えばＤＶＤ等の記録媒体に記録された、あるいは、ネットワークを介して、あるいは放送にて分配された情報の利用に対して課金を行う情報記録／再生装置を含む情報流通システムに関する。

【０００２】

特に、例えばＤＶＤ等の記録媒体に情報を記録する情報記録装置およびＤＶＤ等の記録媒体に記録された情報を再生する情報再生装置に関する。

【０００３】

【従来の技術】

近年、ディジタル情報処理技術や広帯域ＩＳＤＮ等の通信技術の発達、ＤＶＤ等の大容量、高画質、高音質を実現する高度な情報記録媒体の開発が進んでいる。このような情報の伝達手段の多様化、高度化が進むにつれ、ディジタル化された著作物等がネットワーク、記録媒体などを介して利用者の手元に大量に頒布され、利用者がそれらを自由に利用できる環境が生まれつつある。このような環境は、著作物の無断複製、無断改変、著作者の意図しない流通などが起こる機会を増大させるものであり、著作物の権利者にとって、自己

の利益が不当に害されるのではないかという懸念を抱かせるものである。
【０００４】
このような著作物の権利者の懸念を拭い払えるよう、迅速かつ手軽にディジタル化された著作物を流通させるとともに、適正にそれらを利用できるようなディジタル情報の利用環境を提供できる著作権の保護を前提としたシステムの開発は今後の重要な課題となる。
【０００５】
ＤＶＤは、ＣＤ－ＲＯＭに代わる大容量のパソコンメディアであるとともに、映画、音楽、ゲーム、カラオケ等、様々な用途への広がりを期待でき、このようなＤＶＤの普及を図るために、ＤＶＤのタイトル価格を低く抑えたり、レンタルＤＶＤ市場への拡大も予想される。従って、このような観点からも、ＤＶＤ等の記録媒体に記録されたディジタル化された著作物の所有ではなく利用に対して課金するという考えに基づく、情報に対する著作権の保護を前提とした情報の流通システムが不可欠となる。
【０００６】
【発明が解決しようとする課題】
そこで、本発明は、ディジタル化された著作物を迅速かつ手軽に流通させるとともに、著作権の保護を前提としたディジタル情報の利用環境を提供する情報流通システムを構築するための情報記録装置および情報再生装置および課金装置を提供することを目的とする。すなわち、ネットワークあるいは記録媒体を介して分配されたディジタル化された著作物を迅速かつ手軽に流通させるとともに、ディジタル情報の利用に対する課金による著作権の保護を前提としたディジタル情報の利用環境を構築するための情報記録装置およびその記録された情報の再生装置および情報利用に対する課金装置を提供することを目的とする。
【０００７】
【課題を解決するための手段】
（第１の実施形態）
（１）　本発明の情報記録装置（請求項１）は、コンテンツ情報を暗号化する暗号化手段と、
少なくとも前記コンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号する復号鍵とを含む暗号化されたライセンス情報を生成するライセンス情報生成手段と、
前記暗号化手段で暗号化されたコンテンツ情報と前記ライセンス情報生成手段で生成されたライセンス情報とを記録媒体に記録する記録手段と、
を具備する。
【０００８】
また、本発明の情報再生装置（請求項４）は、暗号化されたコンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件および前記コンテンツ情報を復号するための第１の鍵情報を含む暗号化されたライセンス情報とが記録された記録媒体から前記コンテンツ情報を再生する情報再生装置において、
前記ライセンス情報を復号するための第２の鍵情報を記憶する記憶手段と、
この記憶手段に記憶されている第２の鍵情報を用いて前記記録媒体に記録されているライセンス情報を復号する第１の復号手段と、
この第１の復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記第１の復号手段で復号されたライセンス情報に含まれる第１の鍵情報を用いて前記記録媒体に記録されているコンテンツ情報を復号する第２の復号手段と、
を具備する。
【０００９】
本発明の情報記録装置により、暗号化されたコンテンツ情報と該コンテンツ情報の利用条件が不可分になるよう記録媒体に記録される。このような記録媒体に記録されたコンテン

ツ情報を再生するには、ライセンス情報を復号するための正当な復号鍵を具備した情報再生装置のみが行え、しかも復号の際には、必ずライセンス情報に含まれる利用条件を参照してコンテンツ情報の利用の可否を判断するため、コンテンツ情報を不正な利用条件の下で利用する事が不可能となる。従って、該コンテンツ情報の著作権の保護を前提としたディジタル情報を迅速かつ手軽に流通させることができる。

【００１０】

（２）　また、本発明の情報記録装置（請求項２）は、コンテンツ情報から一部の情報を分離する分離手段と、

少なくとも、前記分離手段で分離された前記一部の情報と前記コンテンツ情報の利用を制限するための利用条件とを含む暗号化されたライセンス情報を生成するライセンス情報生成手段と、

このライセンス情報生成手段で生成されたライセンス情報と前記コンテンツ情報の他の一部を記録媒体に記録する記録手段と、

を具備する。

【００１１】

本発明の情報再生装置（請求項５）は、コンテンツ情報の一部と、少なくとも前記コンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報の他の一部を含む暗号化されたライセンス情報とが記録された記録媒体から前記コンテンツ情報を再生する情報再生装置において、

前記ライセンス情報を復号する鍵情報を記憶する記憶手段と、

この記憶手段に記憶されている鍵情報を用いて前記記録媒体に記録されているライセンス情報を復号する復号手段と、

この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる前記コンテンツ情報の一部と、前記記録媒体に記録されている前記コンテンツ情報の一部とを合成して前記コンテンツ情報を再生する再生手段と、

を具備する。

【００１２】

本発明の情報記録装置により、コンテンツ情報と該コンテンツ情報の利用条件が不可分になるよう記録媒体に記録される。このような記録媒体に記録されたコンテンツ情報を再生するには、ライセンス情報を復号するための正当な復号鍵を具備した情報再生装置のみが行え、しかも復号の際には、必ずライセンス情報に含まれる利用条件を参照してコンテンツ情報の利用の可否を判断するため、コンテンツ情報を不正な利用条件の下で利用する事が不可能となる。従って、該コンテンツ情報の著作権の保護を前提としたディジタル情報を迅速かつ手軽に流通させることができる。

【００１３】

（３）　本発明の情報記録装置（請求項３）は、コンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件とを含む暗号化された記録情報を生成する記録情報生成手段と、

この記録情報生成手段で生成された記録情報を記録媒体に記録する記録手段と、

を具備する。

【００１４】

本発明の情報再生装置（請求項６）は、少なくともコンテンツ情報と前記コンテンツ情報の利用を制限するための利用条件とを含む暗号化された記録情報が記録された記録媒体から前記コンテンツ情報を再生する情報再生装置において、

前記記録情報を復号するための鍵情報を記憶する記憶手段と、

この記憶手段に記憶されている鍵情報を用いて前記記録媒体に記録されている記録情報を復号する復号手段と、

この復号手段で復号された記録情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたコンテンツ情報を再生する再生手段と、
を具備する。
【００１５】
本発明の情報記録装置により、コンテンツ情報と該コンテンツ情報の利用条件が不可分になるよう記録媒体に記録される。このような記録媒体に記録されたコンテンツ情報を再生するには、記録情報を復号するための正当な復号鍵を具備した情報再生装置のみが行え、しかも復号の際には、必ず利用条件を参照してコンテンツ情報の利用の可否を判断するため、コンテンツ情報を不正な利用条件の下で利用する事が不可能となる。従って、該コンテンツ情報の著作権の保護を前提としたディジタル情報を迅速かつ手軽に流通させることができる。
【００１６】
（４）　本発明の課金装置（請求項１５）は、記録媒体に記録されたコンテンツ情報の利用に対する課金を行う課金装置において、
記録媒体に記録されたコンテンツ情報の利用条件を入力する入力手段と、
この入力手段で入力された利用条件に基づき前記コンテンツ情報の利用に対する料金の支払いを要求する要求手段と、
前記要求に応じて料金の支払いが確認されたとき、少なくとも前記入力手段で入力された利用条件を含むライセンス情報を前記記録媒体に記録する記録手段と、
を具備することにより、コンテンツ情報およびその利用を制限する利用条件を含むライセンス情報の記録された記録媒体に対し、該コンテンツ情報の利用に対する適切な課金が行えるとともに、該コンテンツ情報の著作権の保護を前提としたディジタル情報を迅速かつ手軽に流通させることができる。
【００１７】
（５）　本発明の課金装置（請求項１６）は、コンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件を含む暗号化されたライセンス情報とが記録された記録媒体を介した前記コンテンツ情報の利用に対する課金を行う課金装置において、
前記記録媒体に記録された暗号化されたライセンス情報を入力する入力手段と、
この入力手段で入力された暗号化されたライセンス情報を復号する復号手段と、
前記コンテンツ情報を利用するための利用条件を入力する利用条件入力手段と、　この利用条件入力手段で入力された利用条件に基づき前記コンテンツ情報の利用に対する料金の支払いを要求する要求手段と、
前記要求に応じて料金の支払いが確認されたとき、前記利用条件入力手段で入力された利用条件に基づき前記復号手段で復号されたライセンス情報を更新する更新手段と、
この更新手段で更新されたライセンス情報を暗号化する暗号手段と、
この暗号手段で暗号化されたライセンス情報を出力する出力手段と、
を具備することにより、コンテンツ情報およびその利用を制限する使用条件を含むライセンス情報の記録された記録媒体に対し、該コンテンツ情報の利用に対する適切な課金が行えるとともに、該コンテンツ情報の著作権の保護を前提としたディジタル情報を迅速かつ手軽に流通させることができる。
（第２の実施形態）
（６）　本発明の判定装置（請求項１７、請求項１８、請求項４９：復号ユニットＡ）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第１の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、
前記ライセンス情報を復号する第２の鍵情報を予め定められた時間毎に生成する鍵生成手段と、
入力された前記ライセンス情報を前記鍵生成手段で生成された第２の鍵情報を用いて復号

する復号手段と、
この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第１の鍵情報を出力する出力手段と、
を具備する。
【００１８】
本発明によれば、ラインセンス情報を復号するための秘密鍵（第２の鍵情報）を復号ユニットＡ内で所定タイミング毎に生成し、これをある所定期間に限って用いるようになっているため、コンテンツ情報の利用条件やコンテンツ情報の復号鍵を含むライセンス情報の情報セキュリティの向上が図れる。
【００１９】
（７）　本発明の判定装置（請求項１９、請求項２０：復号ユニットＢ）は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための暗号化された第１の鍵情報と該暗号化された第１の鍵情報を復号するための第２の鍵情報を生成するために必要な第１の鍵生成情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、
前記ライセンス情報を復号する復号手段と、
この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる暗号化された第１の鍵情報と第１の鍵生成情報とを出力する出力手段と、
を具備する。
【００２０】
本発明によれば、コンテンツ情報を復号する第１の鍵情報は、復号ユニットＢ内では暗号化されたままなので、コンテンツ情報の復号鍵情報の情報セキュリティの向上が図れる。
【００２１】
（８）　本発明の判定装置（請求項２１、請求項２２、請求項５０：復号ユニットＣ）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための暗号化された第１の鍵情報と該暗号化された第１の鍵情報を復号するための第２の鍵情報を生成するために必要な第１の鍵生成情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、
前記ライセンス情報を復号する第３の鍵情報を予め定められた時間毎に生成する鍵生成手段と、
入力された前記ライセンス情報を前記鍵生成手段で生成された第３の鍵情報を用いて復号する復号手段と、
この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる暗号化された第１の鍵情報と第１の鍵生成情報とを出力する出力手段と、
を具備する。
【００２２】
本発明によれば、ライセンス情報を復号するための秘密鍵（第３の鍵情報）を復号ユニットＣ内で所定タイミング毎に生成し、これを所定期間に限って用いるようになっているため、コンテンツ情報の利用条件やコンテンツ情報の復号鍵を含むライセンス情報の情報セキュリティの向上が図れる。また、コンテンツ情報を復号する第１の鍵情報は、復号ユニットＣ内では暗号化されたままなので、復号鍵情報の情報セキュリティの向上が図れる。
【００２３】

（９） 本発明の判定装置（請求項２３、請求項２４：復号ユニットＤ、復号ユニットＤ’）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第１の鍵情報とを第２の鍵情報で暗号化したものと、少なくとも該第２の鍵情報を生成するために必要な鍵生成情報とを含むライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置において、
入力された前記ライセンス情報に含まれる鍵生成情報に基づき前記第２の鍵情報を生成する鍵生成手段と、
この鍵生成手段で生成された第２の鍵情報を用いて前記ライセンス情報に含まれる利用条件と第１の鍵情報とを復号する復号手段と、
この復号手段で復号された利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号された第１の鍵情報を出力する出力手段と、
を具備する。

【００２４】
本発明によれば、ライセンス情報の暗号化部分（セキュリティ対策を要する重要な情報部分）を復号する第１の鍵情報は、該暗号化部分を復号する際に、その都度生成され、復号後はメモリ上から消去できるため、復号ユニットＤ、Ｄ’内に該第１の鍵情報を保持することがない。従って、利用条件やコンテンツ情報を復号する第１の鍵情報等の重要な情報（第三者には知られて不正利用されては困るような情報）のセキュリティの向上が図れる。

【００２５】
また、ライセンス情報が更新される度に第１の鍵情報（K_{AB}）が異なるので、第１の鍵情報が露見した場合の影響が少なくなる。そればかりか公開鍵暗号に比べ格段に高速である共有鍵暗号が使えるので付加情報のデータサイズを大きくしても実時間で復号し、ライセンス情報に含まれる利用条件に基づくコンテンツの利用可否の反映が行えるという利点がある。

【００２６】
（１０） 本発明の更新装置（請求項２５：復号ユニットＡに対応するライセンス情報更新装置）は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための鍵情報とを含む公開鍵で暗号化されたライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも新たに指定された利用条件と更新された公開鍵とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、
前記更新されたライセンス情報を前記通知された公開鍵で暗号化することを特徴とする。

【００２７】
本発明によれば、ライセンス情報の更新の際には、コンテンツ復号鍵を通知する必要がなく、情報セキュリティの確保されたライセンス情報の更新が可能となる。

【００２８】
（１１） 本発明の更新装置（請求項２６：復号ユニットＢに対応するライセンス情報更新装置）は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための暗号化された第１の鍵情報と該暗号化された第１の鍵情報を復号する第２の鍵情報を生成するために必要な第１の鍵生成情報とを含む暗号化されたライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも新たに指定された利用条件と前記第２の鍵情報を生成するために必要な第２の鍵生成情報とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、
前記利用条件と前記第１の鍵生成情報とを更新し、該更新された第１の鍵生成情報と前記第２の鍵生成情報とに基づき前記第２の鍵情報を更新し、この更新された第２の鍵情報で前記第１の鍵情報を暗号化して、少なくとも該更新された利用条件と該更新された第２の

鍵情報で暗号化された第１の鍵情報と該更新された第１の鍵生成情報とを含む暗号化されたライセンス情報を生成することを特徴とする。

【００２９】

本発明によれば、ライセンス情報の更新の際には、コンテンツ復号鍵を通知する必要がなく、情報セキュリティの確保されたライセンス情報の更新が可能となる。

【００３０】

（１２）　本発明の更新装置（請求項２７：復号ユニットＣに対応するライセンス情報更新装置）は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための暗号化された第１の鍵情報と該暗号化された第１の鍵情報を復号する第２の鍵情報を生成するために必要な第１の鍵生成情報とを含む公開鍵で暗号化されたライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも新たに指定された利用条件と前記第２の鍵情報を生成するために必要な第２の鍵生成情報と更新された公開鍵とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、

前記利用条件と前記第１の鍵生成情報とを更新し、該更新された第１の鍵生成情報と前記第２の鍵生成情報とに基づき前記第２の鍵情報を更新し、この更新された第２の鍵情報で前記第１の鍵情報を暗号化して、少なくとも該更新された利用条件と該更新された第２の鍵情報で暗号化された第１の鍵情報と該更新された第１の鍵生成情報とを含むライセンス情報を生成し、この生成されたライセンス情報を前記通知された公開鍵で暗号化することを特徴とする。

【００３１】

本発明によれば、ライセンス情報の更新の際には、コンテンツ復号鍵を通知する必要がなく、情報セキュリティの確保されたライセンス情報の更新が可能となる。

【００３２】

（１３）本発明の更新装置（請求項２８：復号ユニットＤ、Ｄ’に対応するライセンス情報更新装置）は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための第１の鍵情報とを第２の鍵情報で暗号化したものと、少なくとも該第２の鍵情報を生成するために必要な２つの鍵生成情報とを含むライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも前記２つの鍵生成情報のうちの一方あるいは該一方の鍵生成情報を更新したものと新たに指定された利用条件とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、

前記利用条件と他方の鍵生成情報とを更新し、該更新された他方の鍵生成情報と前記通知された一方の鍵生成情報とに基づき前記第２の鍵情報を更新して、少なくとも該更新された利用条件と該第１の鍵情報とを該更新された第２の鍵情報で暗号化したものと、少なくとも前記通知された一方の鍵生成情報と該更新された他方の鍵生成情報とを含むライセンス情報を生成することを特徴とする。

【００３３】

本発明によれば、ライセンス情報の更新の際には、コンテンツ復号鍵を通知する必要がなく、情報セキュリティの確保されたライセンス情報の更新が可能となる。

【００３４】

（１４）　本発明の情報利用装置（請求項２９：復号ユニットＢ、Ｃに対応する情報利用装置）は、暗号化されたコンテンツ情報を復号するための暗号化された第１の鍵情報と該第１の鍵情報を復号する第２の鍵情報を生成するために必要な第１の鍵生成情報とが入力されて、該コンテンツ情報を復号および利用する情報利用装置において、

前記第１の鍵情報を復号する第２の鍵情報を生成するために必要な第２の鍵生成情報を保持し、この第２の鍵生成情報と前記入力された第１の鍵生成情報とに基づき前記第２の鍵情報を生成し、この生成された第２の鍵情報を用いて前記暗号化されたコンテンツ情報を復号することを特徴とする。

【００３５】

本発明によれば、コンテンツ情報の復号鍵（第１の鍵情報）は暗号化されたまま当該情報利用装置に入力するため、第１の鍵情報を出力する装置（復号ユニットＢ、Ｃ）と当該情報利用装置との間における情報セキュリティの向上が図れる。

（第３の実施形態）

（１５）　本発明の情報利用装置（請求項３０）は、記録媒体に記録された暗号化されたコンテンツ情報を該記録媒体に記憶された、少なくとも前記コンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための第１の鍵情報とを含む暗号化されたライセンス情報に基づき復号および利用する情報利用装置において、

日時を計測する計測手段と、

この計測手段で計測された日時と前記記録媒体に記録されたライセンス情報とに基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

前記判定手段で前記コンテンツ情報の利用が可能と判定されたとき該判定手段から出力される前記第１の鍵情報を用いて前記記録媒体に記録されたコンテンツ情報を復号する復号手段と、

を具備し、

前記計測手段から前記判定手段へ日時を通知するための情報と、前記判定手段から前記復号手段へ出力される第１の鍵情報とは暗号化されていることを特徴とする。

【００３６】

本発明によれば、情報生成装置内の各機能ユニット（計測手段、判定手段、復号手段）間で受け渡しされる情報のセキュリティの向上が図れる。

【００３７】

（１６）　本発明の判定装置（請求項４２）は、暗号化されたコンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件および前記コンテンツ情報を復号するための第１の鍵情報を含む暗号化されたライセンス情報とが記録された記録媒体から読み出された該暗号化されたライセンス情報と、日時を通知するための暗号化された日時情報とを入力して、前記コンテンツ情報の利用の可否を判定する判定装置であって、

前記暗号化されたライセンス情報を復号する第１の復号手段と、

前記暗号化された日時情報を復号する第２の復号手段と、

前記第１および第２の復号手段で復号された情報に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

この判定手段で前記コンテンツ情報の利用が可能と判定されたとき前記第１の鍵情報を暗号化して出力する出力手段と、

を具備し、演算機能を有する携帯可能記録媒体で構成されたことを特徴とする。

【００３８】

本発明の判定装置を例えばパーソナルコンピュータに装着して用いた場合、当該判定装置に入力あるいは出力される情報のセキュリティの向上が図れる。

（第４の実施形態）

（１７）　（請求項５１）請求項１７、１９、２１、２３、２４記載の判定装置において、前記復号手段で復号された前記ライセンス情報には、復号結果の正否を判定するための認証情報が含まれていることにより、時間の経過に従って該ライセンス情報の復号化鍵がいくつも生成される状況であっても、そのうちのいずれか正しい復号鍵で当該ライセンス情報が復号されたか否かを容易に判断できる。

【００３９】

（１８）　本発明の判定装置（請求項５２）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第１の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、

前記ライセンス情報を復号する第２の鍵情報を放送配信される第１の鍵生成情報に基づき生成する鍵生成手段と、

入力された前記ライセンス情報を前記鍵生成手段で生成された第２の鍵情報を用いて復号

する復号手段と、
この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第１の鍵情報を出力する出力手段と、
を具備したことにより、暗号化ライセンス情報の復号化鍵（第２の鍵情報）を生成するために必要なシード情報（第１の鍵生成情報）が放送配信されるので、暗号化ライセンス情報の復号化鍵の更新が容易に行える。
（第５の実施形態）
（１９）本発明の鍵配信装置（請求項５５）は、記録媒体に記録された暗号化されたコンテンツ情報を復号するために必要な第１の鍵情報を前記コンテンツ情報を利用する情報利用装置へ配信する鍵配信装置において、
前記情報利用装置との間で共有される第１の秘密パラメータを記憶する第１の記憶手段と、
この第１の記憶手段に記憶された第１の秘密パラメータと、該情報利用装置との間で交換される第１の公開パラメータとに基づき第２の鍵情報を生成する第１の鍵生成手段と、
少なくとも前記第１の鍵情報を含む暗号化された第１の暗号情報を、前記第１の鍵生成手段で生成された第２の鍵情報で暗号化する暗号手段と、
この暗号手段で暗号化された少なくとも前記第１の暗号情報を含む第２の暗号情報を前記情報利用装置に配信する配信手段と、
を具備したことにより、コンテンツ情報を復号するために必要なディスクキー（第１の鍵情報）を、その配信元（鍵配信装置としてのライセンス作成装置、ライセンス注入装置）から配信先（情報利用装置としてのカードアダプタ、プレーヤ）とで、双方で共有する秘密パラメータから生成される公開してもかまわない公開パラメータを伝達し合い、自分の秘密パラメータと相手からの公開パラメータによって鍵配送を達成するので、盗聴されるかもしれない安全でない通信路であっても安全に鍵配信が行える。
【００４０】
（２０）本発明の判定装置（請求項６１）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第１の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、
前記ライセンス情報の配信装置との間で共有される第１の秘密パラメータを記憶する第１の記憶手段と、
この第１の記憶手段に記憶された第１の秘密パラメータと前記配信装置との間で交換される第１の公開パラメータとに基づき第２の鍵情報を生成する第１の鍵生成手段と、
受信した前記暗号化されたライセンス情報を前記第１の鍵生成手段で生成された第２の鍵情報で復号する第１の復号手段と、
この第１の復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第１の鍵情報を出力する出力手段と、
を具備したことにより、コンテンツ情報を復号するために必要なディスクキー（第１の鍵情報）の配信元（配信装置としてのライセンス作成装置、ライセンス注入装置）との間で共有する秘密パラメータから生成される公開してもかまわない公開パラメータを伝達し合い、自分の秘密パラメータと配信元からの公開パラメータによって鍵配送を達成するので、盗聴されるかもしれない安全でない通信路であっても安全に第１の鍵情報を受け取れる。
【００４１】
（２１）　本発明の情報利用装置（請求項６６）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第１の鍵情報とを含む暗号

化されたライセンス情報に基づき、前記コンテンツ情報を復号および利用する情報利用装置において、
前記ライセンス情報の配信装置との間で共有される第１の秘密パラメータを記憶する第１の記憶手段と、
この第１の記憶手段に記憶された第１の秘密パラメータと前記配信装置との間で交換される第１の公開パラメータとに基づき第２の鍵情報を生成する第１の鍵生成手段と、
受信した前記暗号化されたライセンス情報を前記第１の鍵生成手段で生成された第２の鍵情報で復号する第１の復号手段と、
この第１の復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第１の鍵情報を用いて前記コンテンツ情報を復号することを特徴とする。

【００４２】

本発明によれば、コンテンツ情報を復号するために必要なディスクキー（第１の鍵情報）の配信元（配信装置としてのライセンス作成装置、ライセンス注入装置）との間で共有する秘密パラメータから生成される公開してもかまわない公開パラメータを伝達し合い、自分の秘密パラメータと配信元からの公開パラメータによって鍵配送を達成するので、盗聴されるかもしれない安全でない通信路であっても安全に第１の鍵情報を受け取れる。

【００４３】

（２２）　本発明の記録媒体（請求項７０、７１）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第１の鍵情報とを含む暗号化されたライセンス情報とが記録された演算機能を有する記録媒体であって、
前記ライセンス情報の記録装置との間で共有される第１の秘密パラメータと、前記ライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置（あるいは、前記コンテンツ情報を利用する情報利用装置）との間で共有される第２の秘密パラメータとを記憶する第１の記憶手段と、
予め与えられた識別情報を記憶する第２の記憶手段と、
前記第１の記憶手段に記憶された第１の秘密パラメータと前記記録装置との間で交換される第１の公開パラメータとに基づき第２の鍵情報を生成する第１の鍵生成手段と、
この第１の鍵生成手段で生成された第２の鍵情報を用いて前記識別情報を暗号化する第１の暗号手段と、
前記第１の記憶手段に記憶された第２の秘密パラメータと前記判定装置（あるいは前記情報利用装置）との間で交換される第２の公開パラメータとに基づき第３の鍵情報を生成する第２の鍵生成手段と、
この第２の鍵生成手段で生成された第３の鍵情報を用いて前記識別情報を暗号化する第２の暗号手段と、
前記第１および第２の暗号手段で暗号化された識別情報を前記記録装置および前記判定装置（あるいは前記情報利用装置）に送信する送信手段と、
を具備したことにより、コンテンツ情報を復号するために必要なディスクキー（第１の鍵情報）を、その配信元（記録装置としてのライセンス注入装置）から配信先（判定装置（あるいは情報利用装置）としてのカードアダプタ、プレーヤ）へ配信する記録媒体が、その識別情報を当該配信元および配信先のそれぞれとの間で共有する秘密パラメータから生成される公開してもかまわない公開パラメータを伝達し合い、自分の秘密パラメータと相手からの公開パラメータによって配送するので、盗聴されるかもしれない安全でない通信路であっても安全に当該識別情報の配信が行えるとともに、当該識別情報を有する記録媒体のみがディスクキーを配信するための正当な記録媒体であることを配信元および配信先との間で認識できるので（例えば、配信元にてライセンス情報に当該記録媒体の識別情報を含めることにより、配信先にて、このライセンス情報に含まれる識別情報と、当該ライセンス情報の記録されていた記録媒体の識別情報とが一致していたときにライセンス判定

を行う）、当該記録媒体を介して双方でディスクキーが安全に受け渡しできる。
【００４４】
【発明の実施の形態】
以下、本発明の実施形態について図面を参照して説明する。
（第１の実施形態）
まず、本発明の第１の実施形態に係る情報記録装置および情報再生装置を用いた情報流通システムの全体を概略的に説明する。
【００４５】
本発明に係る情報記録装置および情報再生装置を用いた情報流通システムの構成例を図５３に示す。図５３において、ライセンス情報生成部１００２、情報記録部１００３は、図１、図３、図７等に示したライセンス情報生成部および情報記録部と等価であり、復号ユニット１０１３は、図９、図１２、図２７、図３９、図４３等に示す復号ユニットと等価である。再生部１０１４、読み出し部１０１２も、図８等に示す情報再生装置の再生部、読み出し部と等価である。
【００４６】
図５３に示すシステム全体の動作を以下、簡単に説明する。課金対象情報は暗号鍵ｋｅ（１）によって暗号化されている（［課金対象情報］ｋｅ（１））。先ず、ライセンス情報生部１００２に課金対象情報の復号鍵ｋｄ（１）と利用期限等の利用条件が入力される（ステップＳ７０１、ステップＳ７０２）。
【００４７】
ライセンス情報生成部１００２は複合鍵ｋｄ（１）と利用条件とをマージした後、暗号鍵ｋｅによって暗号化してライセンス情報を生成し、それを情報記録部１００３に送る（ステップＳ７０３）。一方、暗号化された課金対象情報も情報記録部１００３に入力され（ステップＳ７０４）、ライセンス情報と共に情報蓄積部１００４に記録される（ステップＳ７０５）。
【００４８】
情報蓄積部１００４は、ＤＶＤ－ＲＯＭやＤＶＤ－ＲＡＭ、ハードディスク等のメディアである。このメディアに記録された情報が直に、或いは放送やインターネット等を通じて別のメディア（すなわち、情報蓄積部１０１５）に移し替えられて、情報再生装置１０１１の読み出し部１０１２によって読み出される（ステップＳ７０６）。読み出されたライセンス情報は、復号ユニット１０１３に送られる（ステップＳ７０７）。復号ユニット１０１３は、暗号鍵ｋｅに対する復号鍵ｋｄを保持しており、ライセンス情報を復号し、課金対象情報の復号鍵ｋｄ（１）と利用条件とを取り出す。復号ユニット１０１３は利用条件をチェックし、課金対象情報が利用可能か否かを決定する。利用可能であれば、復号ユニットは復号鍵ｋｄ（１）を、再生部１０１４に対して出力する（ステップＳ７０８）。再生部１０１４は、読み出し部１０１２から［課金対象情報］ｋｅ（１）を取り出し（ステップＳ７０９）、復号鍵ｋｄ（１）によって復号し、課金対象情報を再生する。
【００４９】
復号ユニット１０１３は、復号鍵ｋｄと、ライセンス情報の復号を行うアルゴリズムとを保持している。セキュリテイに対する攻撃を避ける為に、復号ユニット１０１３は、ソフトウェアではなく、例えばＩＣチップとして実装する事が望ましい。この場合、復号ユニット１０１３はライセンス情報の入力部と、（利用可能と判断した場合に）課金対象情報の復号鍵を出力する出力部を具備したＩＣチップであり、復号や利用可否の判断は全てチップ内で行われる。
【００５０】
本発明の要点の１つは、ライセンス情報生成部１００２が、課金対象情報の復号鍵ｋｄ（１）と利用条件とをマージした後、暗号化を施す点にある。一般に暗号化は、暗号化対象情報のビットを撹拌する。従って、暗号化処理後は、同時に暗号化された２つの情報を分離する事は（復号による他は）不可能になる。暗号化処理のこの性質を利用して、課金対象情報と利用条件とを分離不可能にする事が重要である。

【００５１】
以上説明した実施形態の場合、課金対象情報は暗号鍵ｋｅ（１）によって暗号化されている。従って、
１．課金対象情報を利用するためには、復号鍵ｋｄ（１）を要する。ところが、復号鍵ｋｄ（１）は、ライセンス情報の一部として、利用条件と不可分に暗号化されている。ライセンス情報と課金対象情報とは分離可能であるが、適正でないライセンス情報は、課金対象情報を正しく復号するための復号鍵を含まないので、ライセンス情報の「すり替え」は意味をなさない。
【００５２】
２．正しい復号鍵ｋｄ（１）を得る為には、適正なライセンス情報を復号しなければならない。ところが、
３．この復号は復号鍵ｋｅを保持する正統的な復号ユニットによってしか、行い得ない。そして、
４．正統的な復号ユニットは、ライセンス情報に含まれる利用条件を必ず参照し、利用の可否を判定する。従って、
５．本発明のライセンス情報生成部および復号ユニットを含む装置においては、課金対象情報を不正な利用条件の下で利用する事が原理的に不可能である。
【００５３】
復号ユニット１０１３が、課金対象情報を利用不可と判定し、復号鍵ｋｄ（１）の出力を行わなかった場合、課金対象情報を利用する為には、ライセンス情報の更新又は有効なライセンス情報の追加を行う他はない。この時点が、情報利用者に対する課金発生のタイミングである。利用者は、店舗や自動販売機、或いはインターネット経由等、何らかの方法でライセンス情報の更新又は新規取得を行わなければならない。店舗に設置された装置や自動販売機、或いはネットワーク・サーバーは、復号鍵ｋｄと暗号化の鍵ｋｅを保持しており、ライセンス情報の復号と情報の書き換え及び再暗号化を行い、ライセンス情報を更新する事ができる。
【００５４】
利用者がライセンス情報の更新（又は新規発行）を受ける為には、当該課金対象情報に付帯するライセンス情報（の１つ）を、ライセンス情報更新機能を有する装置に送らなければならない。
【００５５】
１’．　復号鍵ｋｄと暗号化用の鍵ｋｅとを有する正統的な装置のみが、課金対象情報の復号鍵ｋｄ（１）と利用条件とを復号・分離する事が可能であり、
２’．　復号鍵ｋｄと暗号化用の鍵ｋｅとを有する正統的な装置のみが、利用条件を書き換えた後ライセンス情報として再暗号化する事が出来る。
【００５６】
更新されたライセンス情報は、ライセンス情報更新装置（図２６ライセンス情報更新クライアント部４０３、図３８のライセンス情報更新ユニット６０３、図４１のライセンス情報更新ユニット７０２、図４７のライセンス情報更新ユニット８０４）から出て、利用者の所有するメディアに書き戻される。ライセンス情報更新装置の内部以外の場所では、ライセンス情報は暗号化された状態のままであり、
３’．　本発明に特徴的な暗号化を施されている為、利用条件に対して不正な変更を施す事が不可能である。
【００５７】
一般に、復号用の鍵をネットワークを通じて送信する為に、別の鍵を用いて再び暗号化する等と言う事は、しばしば行われている。しかし、暗号化された課金対象情報を復号する鍵ｋｄ（１）と利用条件とをマージした後に暗号化するという、本発明の特徴は、著作物等の課金対象情報の保護と課金において、上述の様に大きな効果を発揮するものである。
【００５８】
以下、本発明の情報記録装置および情報再生装置および課金装置の構成および動作につい

て、詳細に説明する。
（１）情報記録装置
（１－１）情報記録装置の第１の例
図１は、本発明に係る情報記録装置の第１の構成例を示したものである。すなわち、図１は、ディジタル化された著作物等の課金対象であるコンテンツ情報（以下、課金対象情報と呼ぶ）を暗号化し、その課金対象情報の利用条件と暗号化された課金対象情報を復号するための復号鍵とを暗号化してライセンス情報を生成し、暗号化された課金対象情報およびライセンス情報を所定の記録媒体に記録する情報記録装置の構成例を示したものである。
【００５９】
情報記録装置は、大きく分けて課金対象情報入力部２、ライセンス情報生成部３、記録部８から構成される。
【００６０】
課金対象情報は、暗号鍵ｋｅ（１）を用いて予め暗号化されていて、課金対象情報入力部２に入力される。なお、暗号鍵ｋｅ（１）に対応する復号鍵をｋｄ（１）とする。今後、情報Ｘが暗号鍵Ｋによって暗号化されている事を［Ｘ］ｋと表現することがある。
【００６１】
ライセンス情報生成部３は、利用条件入力部４、復号鍵入力部５、鍵保持部６、暗号化部７から構成される。
【００６２】
鍵保持部６には、暗号鍵ｋｅが予め記憶されている。この暗号鍵ｋｅは、必ずしもｋｅ（１）とは一致しない。
【００６３】
利用条件入力部４には、利用条件が入力する。利用条件とは、課金対象情報の利用期限、ライセンス情報書き込み時刻、コンテンツＩＤ、メディアＩＤあるいは復号ユニットＩＤのうちの少なくとも１つから構成されている。
【００６４】
復号鍵入力部５には、暗号化された課金対象情報を復号するための暗号鍵ｋｅ（１）に対応する復号鍵ｋｄ（１）が入力する。
【００６５】
暗号化部７には、利用条件入力部４、復号鍵入力部５を介して、利用条件、復号鍵ｋｄ（１）がそれぞれ入力し、利用条件と復号鍵ｋｄ（１）がマージされる。
その後、鍵保持部６に記憶されている暗号鍵ｋｅを用いてマージされた利用条件と復号鍵ｋｄ（１）を暗号化する。暗号化の方式としては、一般的に、大きく分けて公開鍵方式と秘密鍵方式があるが、いずれを採用しても良い。ここで暗号化を施されたデータをライセンス情報と呼ぶ。暗号化部７では、マージおよび暗号化により利用条件と復号鍵ｋｄ（１）とを不可分に結び付けることを特徴とする。従って、暗号鍵ｋｅによる暗号を復号できる装置、即ち、暗号鍵ｋｅに対応する復号鍵ｋｄを有する装置のみが、利用条件と復号鍵ｋｄ（１）とを分離する事ができる。復号鍵ｋｄ（１）は、暗号化された課金対象情報を復号するための鍵であるから、結局、課金対象情報と利用条件が不可分に結び付けられることになる。データとして課金対象情報とライセンス情報を分離する事は常に可能である。しかし、適切なライセンス情報なしでは課金対象情報の暗号化を解除してコンテンツを利用する事は出来ないようになっている。
【００６６】
記録部８は、ライセンス情報を情報蓄積部９に書き込み、次いで、その後ろに暗号化された課金対象情報を書き込むようになっている。
【００６７】
情報蓄積部９は、例えば、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ハードディスク等の記録媒体であってもよい。このような情報の記録された記録媒体は、所定の再生装置にセッティングされて情報の再生が行われる。あるいは、情報蓄積部９からインターネット等のネッ

トワークを介して転送され、あるいは放送されて、別の記録媒体に写し替えられ、所定の再生装置で再生されるようになっていてもよい。

【００６８】

図２は、図１の情報記録装置１の動作を説明するためのフローチャートである。まず、暗号化された課金対象情報［課金対象情報］ｋｅ（１）が課金対象情報入力部２に入力され（ステップＳ１）、利用条件が利用条件入力部４に入力され（ステップＳ２）、復号鍵ｋｄ（１）が復号鍵入力部５に入力される（ステップＳ３）。暗号化された課金対象情報は、課金対象情報入力部２から記録部８に転送され（ステップＳ４）、利用条件は利用条件入力部４から暗号化部７に転送され（ステップＳ５）、復号鍵ｋｄ（１）は復号鍵入力部５から暗号化部７に転送される（ステップＳ６）。さらに、鍵保持部６に予め保持されている暗号鍵ｋｅは、暗号化部７に転送される（ステップＳ７）。暗号化部７では、利用条件と復号鍵ｋｄ（１）をマージした後、暗号鍵ｋｅを用いて暗号化してライセンス情報を生成する（ステップＳ８）。そして、生成されたライセンス情報を記録部８に転送する（ステップＳ９）。記録部８は、暗号化された課金対象情報とライセンス情報とをマージして情報蓄積部９に記録する（ステップ１０）。

（１－２）情報記録装置の第２の例

図３は、本発明に係る情報記録装置の第２の構成例を示したものである。すなわち、図３は、ディジタル化された著作物等の課金対象である課金対象情報の一部を利用条件とともに暗号化してライセンス情報を生成し、課金対象情報の残りの部分とライセンス情報を所定の記録媒体に記録する情報記録装置の構成例を示したものである。図１の第１の構成と同様に、課金対象情報と利用条件とを不可分にするために、ここでは、課金対象情報のデータの一部を利用条件と共に暗号化している。

【００６９】

情報記録装置は、大きく分けてデータ分離部１２、ライセンス情報生成部１３、記録部１８から構成される。

【００７０】

データ分離部１２は、課金対象情報を２つに分割する。データ分離部におけるデータの分離例を図５、図６に示す。説明を簡単にするために、静止画の場合について述べるが、動画その他の場合についても同様な方法を利用することができる。

【００７１】

図５に示すように、静止画の一部（図５では、顔の領域）を切り取り、図５（ｂ）に示すような顔の領域部分をライセンス情報の一部として暗号化するようにしてもよい。この場合、ライセンス情報を復号しなくても（即ち、利用料金の支払いを行わなくても）画像を見ることはできるが、その画像は一部を欠いていることになる。また、図６に示すように、画像にフーリエ変換を施し、周波数成分を抽出する。そして、図６（ｂ）に示すような高周波成分をライセンス情報の一部として暗号化するようにしてもよい。この場合、ライセンス情報を復号することができなければ（すなわち、利用料金を払わなければ）、図６（ａ）に示すような周波数成分の画像を再生しても、不鮮明な映像しか得られない。

【００７２】

ライセンス情報生成部１３は、利用条件入力部１４、暗号化部１７、鍵保持部１６から構成される。

【００７３】

鍵保持部１６には、暗号鍵ｋｅが予め記憶されている。

【００７４】

利用条件入力部１４には、利用条件が入力する。利用条件とは、課金対象情報の利用期限、ライセンス情報書き込み時刻、コンテンツＩＤ、メディアＩＤあるいは復号ユニットＩＤのうちの少なくとも１つから構成されている。

【００７５】

暗号化部１７には、利用条件入力部１４を介して利用条件が入力し、データ分離部１２からは課金対象情報を２分して得られた課金対象情報の一部のデータが入力し、この利用条

件と課金対象情報の一部のデータをマージした後、鍵保持部１６に記憶されている暗号鍵ｋｅを用いて暗号化して、ライセンス情報を生成する。

【００７６】

記録部１８は、ライセンス情報を情報蓄積部１９に書き込み、次いで、その後ろにデータ分離部１２で２分された課金対象情報の残りのデータを書き込むようになっている。

【００７７】

情報蓄積部１９は、例えば、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ハードディスク等の記録媒体であってもよい。このような情報の記録された記録媒体は、所定の再生装置にセッティングされて情報の再生が行われる。あるいは、情報蓄積部１９からインターネット等のネットワークを介して転送され、あるいは放送されて、別の記録媒体に写し替えられ、所定の再生装置で再生されるようになっていてもよい。

【００７８】

図４は、図３の情報記録装置１１の動作を説明するためのフローチャートである。まず、課金対象情報がデータ分離部１２に入力され（ステップＳ２１）、利用条件が利用条件入力部１４に入力される（ステップＳ２２）。データ分離部１２は、入力された課金対象情報を２分し（ステップＳ２３）、その結果得られた課金対象情報の一部のデータを暗号化部１７に転送し（ステップＳ２４）、課金対象情報の残りのデータを記録部１８に転送する（ステップＳ２５）。また、利用条件は利用条件入力部１４から暗号化部１７に転送され（ステップＳ２６）、暗号鍵ｋｅは鍵保持部１６から暗号化部１７に転送される（ステップＳ２７）。暗号化部１７では、利用条件とデータ分離部１２から転送された課金対象情報の一部のデータをマージしてた後、暗号鍵ｋｅを用いて暗号化してライセンス情報を生成する（ステップＳ２８）。そして、生成されたライセンス情報を記録部１８に転送する（ステップＳ２９）。記録部１８は、データ分離部１２から転送された課金対象情報の一部のデータとライセンス情報とをマージして情報蓄積部１９に記録する（ステップ３０）。

（１－３）情報記録装置の第３の例

課金対象情報と利用条件とを不可分にするためのさらに他の例として、課金対象情報の全体を利用条件と共に暗号化することも考えられる。

【００７９】

図７は、本発明の第１の実施形態に係る情報記録装置の第３の構成例を示したものである。なお、図７において、図３と同一部分には、同一符号を付し、異なる部分について説明する。すなわち、図３のデータ分離部１２が図７では、課金対象情報入力部２に置き換わっていて、課金対象情報入力部２に入力された課金対象情報は、そのまま、暗号化部１７に転送される。暗号化部１７では、課金対象情報の全てと利用条件とをマージした後、暗号鍵ｋｅを用いて暗号化するようになっている。

（１－４）まとめ

以上、説明したように、情報記録装置の第１の例では、暗号化された課金対象情報を復号するための復号鍵ｋｄ（１）と利用条件とをマージし、暗号鍵ｋｅを用いて暗号化してライセンス情報を生成することにより、利用条件と復号鍵ｋｄ（１）とを付加分に結び付けて、暗号化された課金対象情報とライセンス情報とをマージして情報蓄積部９に記録することにより、課金対象情報と利用条件とを不可分に結び付けることができる。この場合、暗号鍵ｋｅに対応する復号鍵ｋｄを有する情報再生装置のみが、利用条件と復号鍵ｋｄ（１）とを分離する事ができ、従って、この分離された復号鍵ｋｄ（１）を用いて、暗号化された課金対象情報を復号・再生することができる。

【００８０】

情報記録装置の第２の例では、課金対象情報の一部のデータと利用条件とをマージし、暗号鍵ｋｅを用いて暗号化してライセンス情報を生成し、残りの課金対象情報の一部のデータとライセンス情報とをマージして情報蓄積部１９に記録することにより、課金対象情報と利用条件とを不可分に結び付けることができる。この場合、暗号鍵ｋｅに対応する復号鍵ｋｄを有する情報再生装置のみが、課金対象情報の一部のデータと利用条件とを復号・

分離する事ができ、従って、この復号・分離された課金対象情報の一部のデータと残りのデータとから課金対象情報を再生することができる。

【００８１】

情報記録装置の第３の例では、課金対象情報の全データと利用条件とをマージし、暗号鍵ｋｅを用いて暗号化して情報蓄積部１９に記録することにより、課金対象情報と利用条件とを不可分に結び付けることができる。この場合、暗号鍵ｋｅに対応する復号鍵ｋｄを有する情報再生装置のみが、課金対象情報のデータと利用条件とを復号・分離・再生することができる。

【００８２】

これらのいずれも、復号によらずしては、課金対象情報と利用条件とを分離できない様にする為の仕組みを与えるものである。

【００８３】

また、情報蓄積部９、１９は、例えば、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ハードディスク等の記録媒体であってもよい。このような情報の記録された記録媒体は、所定の再生装置にセッティングされて情報の再生が行われる。あるいは、情報蓄積部９、１９からインターネット等のネットワークを介して転送され、あるいは放送されて、別の記録媒体に写し替えられ、所定の再生装置で再生されるようになっていてもよい。

（２）情報再生装置

（２－１）情報再生装置の第１の例

図８は、本発明に係る情報再生装置の第１の構成例を示したものである。すなわち、図８は、前述の図１の第１の情報記録装置、図３の第２の情報記録装置、図７の第３の情報記録装置で、情報蓄積部９あるいは情報蓄積部１９に記録された情報を記録媒体あるいはネットワークあるいは放送にてユーザ分配し、その分配された情報を再生する情報再生装置の構成例を示したものである。

【００８４】

例えば、第１の情報記録装置で情報蓄積部９に記録された情報の１単位は、暗号化された課金対象情報と、それを復号する復号鍵ｋｄ（１）と利用条件とを暗号鍵ｋｅを用いて暗号化して生成されたライセンス情報とをマージしたものである。

【００８５】

利用条件には、例えば、利用期限が含まれている。利用期限とは、たとえば、ユーザが所定の料金を支払った場合に、その料金に見合った課金対象情報の利用期限である。また利用条件には、ライセンス情報記録時刻が含まれていてもよい。ライセンス情報記録時刻とは、例えば、図１の第１の情報記録装置でライセンス情報が情報蓄積部９に記録された時刻、より具体的には、ライセンス情報生成部３でのライセンス情報生成時に、例えば、利用条件入力部４に具備される時計から読みとられた時刻情報である。

【００８６】

図８において、情報再生装置は大きく分けて、情報蓄積部１０１、読み出し部１０２、復号ユニット１０３、再生部１０４から構成される。

【００８７】

情報蓄積部１０１は、例えば、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ハードディスク等の記録媒体であってもよい。また、情報蓄積部１０１に記録されている情報は、図１、図３、図７の情報蓄積部９あるいは情報蓄積部１９に記録された情報がインターネット等のネットワークを介して転送され、あるいは放送されて、写し替えられたものであってもよい。

【００８８】

読み出し部１０２は、情報蓄積部１０１から１単位の情報を読み出し、ライセンス情報を復号ユニット１０３へ転送し、暗号化された課金対象情報を再生部１０４にそれぞれ転送する。

【００８９】

復号ユニット１０３は、予め記憶する復号鍵ｋｄを用いてライセンス情報を復号し、その結果得られた利用条件に基づき、暗号化された課金対象情報を復号する復号鍵ｋｄ（１）

を再生部１０４に出力するか否かを判定することにより、著作権保護を行うようになっている。

【００９０】

課金対象情報は、暗号鍵ｋｅ（１）によって暗号化されているため、再生部１０４に暗号鍵ｋｅ（１）に対応する復号鍵ｋｄ（１）が与えられない限り、課金対象情報を再生することはできない。復号鍵ｋｄ（１）は、復号ユニット１０３から再生部１０４に転送されるようになっている。なお、復号鍵ｋｄ（１）を復号ユニット１０３から再生部１０４へ転送する際には、通常保護される。復号鍵ｋｄ（１）を転送中に取得・保存されると、その後は、復号ユニット１０３を経由しなくても再生が可能になってしまう。それでは復号ユニット１０３における利用条件チェック等の著作権保護が無意味になるからである。転送保護の具体的な方法としては、例えば、「日経エレクトロニクス」１９９６．１１．１８（Ｎｏ．６７６）ニュースレポート（ｐ１３－ｐ１４）に、その一例を見る事ができる。

【００９１】

再生部１０４は、復号部１０５を具備している。復号部１０５では、読み出し部１０２から転送された暗号化された課金対象情報を、復号ユニット１０３から転送された復号鍵ｋｄ（１）を用いて復号する。再生部１０４では、復号部１０５で復号した結果得られた課金対象情報のデータを表示するための予め定められたデコードを施し、所定の表示装置に表示するようになっている。

【００９２】

復号ユニット１０３の構成例を図９に示す。復号ユニット１０３は、ライセンス情報入力部１０３ａ、復号部１０３ｂ、復号鍵保持部１０３ｃ、判定部１０３ｄ、時計参照部１０３ｅ、時計１０３ｆから構成される。

【００９３】

ライセンス情報入力部１０３ａは、読み出し部１０２から転送されたライセンス情報を受け取ると、それを復号部１０３ｂに出力する。

【００９４】

復号部１０３ｂでは、復号鍵保持部１０３ｃに予め記憶されている復号鍵ｋｄを用いてライセンス情報を復号し、その結果得られた利用条件、すなわち、利用期限と、復号鍵ｋｄ（１）を判定部１０３ｄに出力する。

【００９５】

時計参照部１０３ｅは、時計１０３ｆで示されている時刻（時計時刻）を読みとるようになっている。

【００９６】

判定部１０３ｄは、時計参照部１０３ｅから取得した時計時刻（現在時刻を示す）と、利用期限とを比較して、時計時刻≦利用期限である時、課金対象情報の利用可と判断し（すなわち、復号鍵ｋｄ（１）の出力を可と判定し）復号鍵ｋｄ（１）を再生部１０４に出力する。

【００９７】

利用条件にさらに、ライセンス情報記録時刻が含まれている場合、利用期限のチェックとライセンス情報記録時刻のチェックも行う。すなわち、判定部１０３ｄは、利用期限が有効であるとき、時計時刻とライセンス情報記録時刻を比較し、さらに、時計時刻≧ライセンス情報記録時刻が成立する時、復号鍵ｋｄ（１）を再生部１０４に出力する。このチェックは「ライセンス情報が記録されたのは過去である」と言う当然の事柄を確認しているだけであるが、重要な意味を持っている。すなわち、時計参照部１０３ｅにて参照する時計１０３ｆは、常に正確であるとは限らない。特に、時計が極端に遅れることは、利用期限の遵守の観点から、好ましくない。ライセンス情報記録時刻に関する上記のチェックは、時計の遅れに一定の歯止めをかける意味を持っている。例えば、時計が１ヶ月前の時刻を指していたとする。ライセンス情報記録時刻がある日の１２：００で、利用期限がその丁度１週間後の１２：００であったとする。ライセンス情報記録時刻のチェックを行わな

い場合、利用者は１週間＋１ヶ月の課金対象情報利用が可能になってしまう。ライセンス情報記録時刻のチェックを行う事により、時計が極めて遅れている場合の課金対象情報の利用を禁止する事ができる。

【００９８】

図１０に示すフローチャートは、図８の情報再生装置の処理動作の流れを説明するためのものである。読み出し部１０２は、情報蓄積部１０１に記録されている１単位の情報、すなわち、暗号化された課金対象情報とライセンス情報を読み出すと（ステップＳ４１）、ライセンス情報を復号ユニット１０３へ転送し（ステップＳ４２）、暗号化された課金対象情報を再生部１０４へ転送する（ステップＳ４３）。復号ユニット１０３では、予め記憶している復号鍵ｋｄを用いてライセンス情報を復号し、利用条件（利用期限）と復号鍵ｋｄ（１）を得る。そして、利用条件（利用期限）に基づき課金対象情報の利用の可否を判断する（ステップＳ４４）。利用期限が有効で課金対象情報の利用が可と判断されたとき（ステップＳ４５）、復号ユニット１０３は、復号鍵ｋｄ（１）を再生部１０４に転送する（ステップＳ４６）。一方、課金対象情報の利用が不可と判断されたときは、復号鍵ｋｄ（１）の出力不可通知を再生部１０４に出力し、処理を終了する。再生部１０４では、復号鍵ｋｄ（１）を用いて暗号化された課金対象情報を復号し、さらにデコードして課金対象情報を再生する（ステップＳ４７）。

【００９９】

次に、図１１に示すフローチャート、図８、図９を参照して、図１０のステップＳ４４～Ｓ４６の復号ユニット１０３の処理動作の流れをより詳細に説明する。復号ユニット１０３のライセンス情報入力部１０３ａは、読み出し部１０２から転送されてきたライセンス情報を受け取ると（ステップＳ５１）、ライセンス情報を復号部１０３ｂに転送する（ステップＳ５２）。復号鍵保持部１０３ｃから復号鍵ｋｄが転送されると（ステップＳ５３）、復号部１０３ｂでは復号鍵ｋｄを用いてライセンス情報を復号する（ステップＳ５４）。ライセンス情報を復号した結果得られたデータは、判定部１０３ｄに転送される（ステップＳ５５）。時計参照部１０３ｅから時計時刻が転送されてくると（ステップＳ５６）、判定部１０３ｄは、利用条件（利用期限）と時計時刻を比較して課金対象情報の利用の可否（すなわち、復号鍵ｋｄ（１）を再生部１０４に出力するか否か）を判定する（ステップＳ５７）。課金対象情報の利用が可と判定されたときは、復号鍵ｋｄ（１）を再生部１０４に出力し（ステップＳ５８～Ｓ５９）、課金対象情報の利用が不可と判定されたときは、再生部１０４に復号鍵ｋｄ（１）の出力不可通知を出力する（ステップＳ５８、ステップＳ６０）。

（２－２）復号ユニットの構成および復号ユニットに具備される時計

利用条件として課金対象情報の利用期限を用い、課金対象情報の利用期限限定を行う場合、図９の復号ユニット１０３に具備される時計１０３ｆの正確さは重要である。その意味で、ユーザが任意に時刻設定を行う事を不可能にする仕組みが必要である。図１２に、その様な仕組みを有した復号ユニットの構成例を示す。なお、図１２において、図９と同一部分には同一符号を付している。

【０１００】

図１２に示すように、時計１０３ｆは、時刻設定部１１１、時刻設定無効化部１１２、計時カウンタ１１３から構成される。図１３に示すフローチャートを参照して、図１２の時計１０３ｆの動作を説明する。工場出荷時に設定時刻情報を含む時刻設定指示情報を時計設定部１１１を介して入力すると（ステップＳ７１）、時計設定部１１１は、その指示された設定時刻を計時カウンタ１１３に設定する（ステップＳ７２～ステップＳ７３）。その後、時刻設定無効化部１１２にて、以後の時刻設定部１１１を介しての時刻設定が無効となるような処置を施す（ステップＳ７４～ステップＳ７５）。時刻設定無効化部１１２は、例えば、時刻設定部１１１と計時カウンタ１１３を結ぶ回路に過電流を流して、時刻設定部１１１と計時カウンタ１１３を物理的に遮断するようにしてもよい。時刻設定無効化処置を施された後は、時刻設定は一切不可能になる。

【０１０１】

誤差評価部１０３ｇは、最大累積誤差を、例えば、次の様な方法で決定する。誤差評価部は、時計１０３ｆの「最大遅れ時」と「最大進み時」を保持している。また、誤差評価用の計時カウンタを具備し、この計時カウンタで毎時最大遅れ、最大進みをそれぞれ加算して、その加算値である累積最大遅れと累積最大進み（これらをまとめて累積誤差と呼ぶ）とを判定部１０３ｄに転送する。

【０１０２】

累積最大進み、累積最大遅れとは、例えば、時計１０３ｆ自体の動作異常により生じる誤差の累積時間である。従って、時計１０３ｆにて示される時計時刻と利用期限およびライセンス情報記録時刻とをそれぞれ比較する際には、この累積誤差を加味する必要がある。

【０１０３】

この場合、復号ユニット１０３の判定部１０３ｄは、次式の成立を調べる。

【０１０４】

時計時刻　≦　利用期限＋累積最大進み

時計時刻　≧　ライセンス情報記録（更新）時刻－累積最大遅れ

この２式が同時に成立する時、課金対象情報の利用を可と判定する。第１の情報記録装置により情報蓄積部９に記録された情報を再生する場合には、復号鍵ｋｄ（１）、第２の情報記録装置により情報蓄積部１９に記録された情報を再生する場合は、課金対象情報の一部の出力をぞれぞれ可と判定する。

【０１０５】

次に、図１４に示すフローチャートを参照して、図１２の復号ユニットの処理動作について説明する。復号ユニット１０３のライセンス情報入力部１０３ａは、読み出し部１０２から転送されてきたライセンス情報を受け取ると（ステップＳ８１）、ライセンス情報を復号部１０３ｂに転送する（ステップＳ８２）。復号鍵保持部１０３ｃから復号鍵ｋｄが転送されると（ステップＳ８３）、復号部１０３ｂでは復号鍵ｋｄを用いてライセンス情報を復号する（ステップＳ８４）。ライセンス情報を復号した結果得られたデータは、判定部１０３ｄに転送される（ステップＳ８５）。時計参照部１０３ｅが時計１０３ｆから時計時刻を取得し（ステップＳ８６）、その取得した時計時刻を判定部１０３ｄに転送する（ステップＳ８７）。判定部１０３ｄは、さらに、誤差評価部１０３ｇから累積誤差を取得すると（ステップＳ８８）、時計１０３ｆの累積誤差を加味して、利用条件（利用期限）と時計時刻との比較を行い、課金対象情報の利用の可否（すなわち、復号鍵ｋｄ（１）を再生部１０４に出力するか否か）を判定する（ステップＳ８９）。課金対象情報の利用が可と判定されたときは、復号鍵ｋｄ（１）を再生部１０４に出力し（ステップＳ９０～Ｓ９１）、課金対象情報の利用が不可と判定されたときは、再生部１０４に復号鍵ｋｄ（１）の出力不可通知を出力する（ステップＳ９０、ステップＳ９２）。

（２－３）復号ユニットに具備された時計の時刻設定：その１

図１５は、復号ユニット１０３に具備される時計１０３ｆの他の構成例を示したもので、暗号化された時刻設定指示情報に基づき時刻設定を行う時計１０３ｆの構成例を示したものである。

【０１０６】

図１５に示すように、時計１０３ｆは、設定時刻入力部１２１、復号部１２２、コマンド認証部１２３、時刻設定部１２４、計時カウンタ１２５から構成される。

【０１０７】

このような構成の時計１０３ｆの動作について図１６に示すフローチャートを参照して説明する。設定時刻情報を含む時刻設定指示情報は予め暗号化され、その暗号化された時刻設定指示情報が設定時刻入力部１２１に入力されると（ステップＳ１０１）、設定時刻入力部１２１は、暗号化された時刻設定指示情報を復号部１２２へ転送する（ステップＳ１０２）。復号部１２２は、暗号化された時刻設定指示情報を復号し（ステップＳ１０３）、その復号された時刻設定指示情報をコマンド認証部１２３へ転送する（ステップＳ１０４）。コマンド認証部１２３は、時刻設定指示情報のコマンド形式を確認し（ステップＳ１０５）、正しい形式であるときは（ステップＳ１０６）、時刻設定指示情報に含まれる

設定時刻情報を時刻設定部１２４へ転送する（ステップＳ１０７）。時刻設定部１２４は、設定時刻情報に従って計時カウンタ１２５の時刻設定を行う（ステップＳ１０８）。

【０１０８】

時計１０３ｆが図１５に示した構成であることにより、時計１０３ｆに入力される時刻設定指示情報は常に所定の暗号鍵を用いて暗号化されている必要があるため、暗号化を行うことのできない装置（即ち、暗号化用の鍵を保持していない装置）を用いて、時刻設定を行う事は不可能となる。従って、ユーザが安易に時計１０３ｆの時刻設定を行うこともできない。

（２－４）復号ユニットに具備された時計の時刻設定：その２

次に、ネットワークを介して復号ユニット１０３に具備される時計１０３ｆの時刻設定を行う場合について説明する。

【０１０９】

図１７は、ネットワーク時刻設定の概念図である。時刻設定クライアントは，時刻設定を行うべき時計、すなわち、例えば、図８に示すような第１の情報再生装置の復号ユニット１０３に具備される時計１０３ｆを含んでいる。この時計の時刻をここでは、クライアント時刻と呼ぶことにする。時刻設定サーバも内部に時計を具備し、その時計の示す時刻をここでは、サーバ時刻と呼ぶことにする。このような形態にて、ネットワークを介して時刻設定サーバが時刻設定クライアントの具備する時計の時刻設定を行うわけである。

【０１１０】

復号ユニットに具備された時計の時刻設定の際には、若干込み入った処理が必要である。それは、以下の様な理由による。クライアントの時計２０１の進み方のチェックを行わなくてはならない。クライアント時刻の１分が、サーバ時刻の１分に、ほぼ等価である事を確認する作業が必要である。この事は、ｉ）サーバが認証情報の送信時刻を指定する事、ｉｉ）認証情報到着時刻を指定する事（タイムアウトの設定）により、この確認が行われている。なお、クライアントからサーバに認証情報を送信するのは、虚偽の申告を避ける為である。すなわち、サーバは、認証情報の到着時刻を用いて、クライアント時刻の進み具合を計測しているからである。また、サーバから送信される時刻設定コマンドが、クライアントに到着後、速やかに時計２０１に入力される事を保証する必要がある。この事を保証する為に、クライアントの時計２０１にはタイムアウト（時刻設定指示受信時刻）が設けられている。

【０１１１】

時刻設定クライアントの構成例を図１８に示す。図１８に示すように、時刻設定クライアントは時計２０１、ネットワーク通信部２０２、クライアント認証鍵格納部２０３、暗号化部２０４から構成される。

【０１１２】

時刻設定サーバの構成例を図１９に示す。

【０１１３】

次に、時刻設定クライアントおよび時刻設定サーバの動作を示す図２０～図２２のフローチャート、時刻設定クライアントの時計２０１の構成例を示した図２３、およびその動作を示した図２４～図２５のフローチャートを参照して、ネットワークを介して時刻設定サーバから時刻設定クライアントの時計２０１の時刻設定を行う動作について説明する。

【０１１４】

先ず、時刻設定クライアントでは、時計２０１にて示されている現在のクライアント時刻ｔ１をネットワーク通信部２０２を介して、時刻設定サーバに送る（図２０のステップＳ１１１～ステップＳ１１２）。すなわち、図２３に示すように、時刻読み出し部３０２は計時カウンタ３０１から現在のクライアント時刻ｔ１を読み出し（図２４のＳ１６１）、それを図１８のネットワーク通信部２０２へ出力する（図２４のステップＳ１６２）。

【０１１５】

時刻設定サーバでは、ネットワーク接続部２１１を介してクライアント時刻ｔ１を受信すると（図２１のステップＳ１３１）、それを時刻指定部２１２に転送し（ステップＳ１３

２）、時刻指定部２１２は、到着期限時刻設定部２１３にクライアントからの時刻ｔ１の到着を通知するとともに（ステップＳ１３３）、ｔ１に、予め定められた数値を加えて、認証情報送信時刻（クライアント時刻）ｔ２を決定し（ステップＳ１３４）、それをネットワーク接続部２１１を介して時刻設定クライアントに転送する（ステップＳ１３５）。また、認証情報送信時刻ｔ２は指定時刻格納部２１８に格納される（ステップＳ１３６）。到着期限時刻設定部２１３では、時刻到着通知を受け取ると、時計２１４から、クライアントからの時刻ｔ１の到着時刻（サーバ時刻）Ｔ１を取得し（ステップＳ１３７）、Ｔ１に、予め定められた数値を加えて、認証情報到着時刻（サーバ時刻）Ｔ２を決定し（ステップＳ１３８）、それを到着期限時刻格納部２１５に格納する（ステップＳ１３９）。

【０１１６】

時刻設定クライアントでは、ネットワーク通信部２０２を介して認証情報送信時刻ｔ２を受信すると（図２０のステップＳ１１３）、それを時計２０１に転送し（ステップＳ１１４）、クライアント時刻ｔ２まで待つ。クライアント時刻で示されるｔ２に、時計２０１は、認証情報を読み出して、時計２０１は、暗号化部２０４に出力する。このとき、認証情報は、時刻「ｔ２」であってもよい（ステップＳ１１５）。すなわち、時計２０１では、図２３に示すように、認証情報送信時刻ｔ２を受け取ると、指定時刻格納部３０３にそれを格納する（図２４のステップＳ１６３）。時刻比較部３０４では、指定時刻格納部３０３に格納された認証情報送信時刻ｔ２を読み出し、さらに、計時カウンタ３０１の示すクライアント時刻ｔを随時参照して、ｔ２とｔとの比較を行い、これらが一致したとき、時刻読み出し部３０２へクライアント時刻の読み出しを指示する（図２４のステップＳ１６４～ステップＳ１６８）。この指示を受けて、時刻読み出し部３０２は、計時カウンタ３０１の示すクライアント時刻（この場合、時刻ｔ２）を読み出し、図１８の暗号化部２０４に出力する（図２４のステップＳ１６９）。さらに、時刻設定クライアントの時計２０１は、ｔ２に、予め定められた数値を加え、時刻設定指示受信時刻（クライアント時刻）ｔ３を決定し、それを時刻設定指示受信時刻格納部３０９に格納する（図２４のステップＳ１７０）。

【０１１７】

時刻設定クライアントの暗号化部２０４では、クライアント認証鍵格納部２０３から暗号鍵ｋ’ｓが転送されてくると（ステップＳ１１６）、認証情報としての時刻「ｔ２」を暗号鍵ｋ’ｓを用いて暗号化し（ステップＳ１１７）、暗号化された認証情報（［ｔ２］ｋ’ｓ）をネットワーク通信部２０２を介して時刻設定サーバに転送する（ステップＳ１１８～ステップＳ１１９）。なお、時刻設定サーバでは、暗号鍵ｋ’ｓに対応する復号鍵ｋ’ｐをサーバ認証鍵格納部２１９に保持しているものとする。

【０１１８】

一方、時刻設定サーバでは、時刻設定クライアントからの暗号化された認証情報をネットワーク接続部２１１を介して受信すると（ステップＳ１４０）、それを到着期限時刻確認部２１６に転送する（ステップＳ１４１）。到着期限時刻確認部２１６は、先に到着期限時刻格納部２１５に格納した認証情報到着時刻Ｔ２を取り出し、暗号化された認証情報を受信した時刻Ｔ（サーバー時刻）を時計２１４から読み出す（ステップＳ１４２～ステップＳ１４４）。そして、認証情報の受信時刻Ｔと認証情報到着時刻Ｔ２とを比較する。Ｔ＞Ｔ２であれば、遅延時間が長すぎると判断し、以後の処理を行わない（ステップＳ１４５）。Ｔ≦Ｔ２ならば、暗号化された認証情報を復号部２１７に転送し（図２２のステップＳ１４６）、サーバ認証鍵格納部２１９に格納されている復号鍵ｋ’ｐを用いて復号し（ステップＳ１４７～ステップＳ１４８）、復号された認証情報を指定時刻確認部２２０に転送する（ステップＳ１４９）。指定時刻確認部２２０には、さらに、先に指定時刻格納部２１８に格納された認証情報送信時刻ｔ２も転送され、これらを比較することにより、時刻設定クライアントの時計の認証を行う（ステップＳ１５０～ステップＳ１５２）。ここでは、時刻「ｔ２」を確認する事になる。時刻設定クライアントの時計の認証に失敗すれば、以後の処理を行わない。時刻設定クライアントの時計の認証に成功すると、指定時刻確認部２２０は、時刻設定指示生成部２２１に対し時刻設定指示を送信する（ステッ

プＳ１５３）。この指示を受けて、時刻設定指示生成部２２１２は、時計２１４からその時点におけるサーバ時刻を読み出し、そのサーバ時刻を含む時刻設定コマンドを生成する。さらに、時刻設定コマンドに、暗号鍵ｋ’ｔによる暗号化を施す。時刻設定クライアントの時計では、暗号鍵ｋ’ｔに対応する復号鍵ｋ’ｑを保持しているものとする（ステップＳ１５４～ステップＳ１５５）。暗号化された時刻設定コマンドはネットワーク接続部２１１を介して時刻設定クライアントに送信される（ステップＳ１５６～ステップＳ１５７）。

【０１１９】

時刻設定クライアントでは、ネットワーク通信部２０２を介して暗号化された時刻設定コマンドを受信すると、それを時計２０１に入力する（図２０のステップＳ１２０～ステップＳ１２１）。

【０１２０】

時計２０１は、図２３に示すように、暗号化された時刻設定コマンドを設定時刻入力部３０５で受け取ると、その旨を時刻設定指示入力時刻参照部３１０に通知する（図２４のステップＳ１７１～ステップＳ１７２）。この通知を受けて、時刻設定指示入力時刻参照部３１０は、計時カウンタ３０１からクライアント時刻ｔを取得し、それを時刻比較部３１１に出力する（図２４のステップＳ１７３～ステップＳ１７４）。時刻比較部３１１は、時刻設定指示受信時刻格納部３０９から先に格納された時刻設定指示受信時刻ｔ３を読み出し、そのときのクライアント時刻ｔと比較する。このとき、時刻比較部３１１は、許容遅延時間格納部３１２に予め格納されている許容遅延時間Δｔを用いて比較判断を行うようにしてもよい（図２４のステップＳ１７５～ステップＳ１７７）。ｔ＞ｔ３＋Δｔであれば、遅延時間が長すぎると判定し、以後の処理を行わない（図２４のステップＳ１７８）。ｔ≦ｔ３ならば、時刻比較部３１１は、設定時刻入力部３０５に対し時刻設定許可を通知する（図２４のステップＳ１７８～ステップＳ１７９）。

この通知により、時刻設定クライアントの時計２０１は、時刻設定サーバから送信された時刻設定指示（コマンド）に基づいて時刻設定動作を行う。

【０１２１】

図２３に示すように、時刻設定クライアントの時計２０１の設定時刻入力部３０５は、時刻設定許可通知を受け取ると、暗号化された時刻設定指示を復号部３０６に転送する（図２５のステップＳ１８０）。復号部３０６は、暗号化された時刻設定指示を復号鍵ｋ’ｑを用いて復号し、復号された時刻設定指示をコマンド認証部３０７へ転送する（図２５のステップＳ１８１～ステップＳ１８２）。コマンド認証部３０７は、時刻設定指示のコマンド形式を適否を確認し、正しいコマンド形式の場合は、時刻設定指示中のサーバ時刻を時刻設定部３０８に転送する（図２５のステップＳ１８３～ステップＳ１８５）。時刻設定部３０８は、計時カウンタの示すクライアント時刻をコマンド認証部３０７から受け取ったサーバ時刻に合わせる（図２５のステップＳ１８６）。

（２－５）情報再生装置の第２の例：ライセンス情報の更新（利用条件に課金対象情報ＩＤを含む）

課金対象情報には、それぞれを識別するための課金対象情報ＩＤが付されていて、利用条件には少なくとも、利用期限と課金対象情報ＩＤを含むものとする。このような条件のもと、情報再生装置の情報蓄積部に既に格納されているライセンス情報をネットワークを介して更新する場合について説明する。

【０１２２】

図２６は、第２の情報再生装置の構成例とライセンス情報を更新するためのシステム全体の構成例を示したもので、第２の情報再生装置は、情報蓄積部４０１、復号ユニット４０３、ライセンス情報更新クライアント部４０３、再生部４０４、ネットワーク接続部４０５、電子決済部４０６から構成される。

【０１２３】

情報再生装置の情報蓄積部４０１は、図８の第１の情報再生装置の情報蓄積部１０１と同様である。情報蓄積部４０１から、図２６では省略されている情報読み出し部にて読み出

された１単位の情報のうち、ライセンス情報は復号ユニット４０２に送られる。

【０１２４】

図２７は、図２６の復号ユニット４０２の構成例を示したものである。なお、図９と同一部分には同一符号を付し、図９に示した構成とは、利用条件に含まれている課金対象情報ＩＤを出力するための課金対象情報ＩＤ出力部１０３ｇが追加されている点で異なる。

【０１２５】

次に、図２８に示すフローチャートを参照して、図２７の復号ユニットの動作について説明する。ライセンス情報は、まず、復号ユニット４０２のライセンス情報入力部１０３ａに入力し、復号部１０３ｂへ送られる（ステップＳ２０１～ステップＳ２０２）。復号部１０３ｂでは、復号鍵保持部１０３ｃに保持されている復号鍵ｋｄを用いてライセンス情報を復号し、復号されたライセンス情報を判定部１０３ｄに転送する（ステップＳ２０３～ステップＳ２０５）。時計参照部１０３ｅから時計時刻が転送されてくると（ステップＳ２０６）、判定部１０３ｄは、利用条件（利用期限）と時計時刻を比較して課金対象情報の利用の可否（すなわち、復号鍵ｋｄ（１）を再生部４０４に出力するか否か）を判定する。課金対象情報の利用が可と判定されたときは、復号鍵ｋｄ（１）を再生部４０４に出力する（ステップＳ２０６～Ｓ２０９）。ここまでは、図９の復号ユニットの動作と同様である。一方、判定部１０３ｄで、課金対象情報の利用が不可と判定されたときは、利用条件に含まれる課金対象情報ＩＤを課金対象情報ＩＤ出力部１０３ｇに転送するとともに、再生部４０４へ復号鍵ｋｄ（１）の出力不可通知を出力する（ステップＳ２１０～ステップＳ２１１）。課金対象情報ＩＤ出力部１０３ｇは、課金対象情報ＩＤをライセンス情報更新クライアント部４０３に出力する（ステップＳ２１２）。

【０１２６】

次に、ライセンス情報更新クライアント部４０３の構成および動作について、主に、図２９および図３０を参照して説明する。復号ユニット４０２から送られてくる課金対象情報ＩＤは、ライセンス情報入力部４０３ａに入力される（ステップＳ２２１）。このとき、課金対象情報ＩＤ以外のライセンス情報をライセンス情報入力部４０３ａに入力するようになっていてもよい。以下、ライセンス情報入力部４０３ａには、少なくとも課金対象情報ＩＤを含むライセンス情報が入力されるものとする。さて、ライセンス情報入力部４０３ａに入力されたライセンス情報は、ライセンス情報転送部４０３ｂを経由してネットワーク接続部４０５に出力され、図２６のライセンス情報更新サーバ４０７に送信されるようになっている（ステップＳ２２２～ステップＳ２２３）。なお、ライセンス情報転送部４０３ｂでは、ライセンス情報を暗号化してからネットワーク接続部４０５に出力するようにしてもよい。

【０１２７】

その後、図２６のライセンス情報更新サーバ４０７から、課金対象情報ＩＤに対応して、暗号化された支払い要求（フィールドＩＤを含む）が送信されると、第２の情報再生装置では、暗号化された支払い要求をネットワーク接続部４０５を介して受信し、ライセンス情報更新クライアント部４０３の支払い要求入力部４０３ｃに転送する（ステップＳ２２４）。さらに、暗号化された支払い要求は復号部４０３ｄに転送される（ステップＳ２２５）。復号部４０３ｄでは、暗号化された支払い要求を復号してから、支払い確認部４０３ｅへ転送する（ステップＳ２２６～ステップＳ２２７）。支払い確認部４０３ｅは、ユーザに対し、例えば、所定の表示装置に支払い要求の内容を表示して、課金対象情報を利用するための料金支払いの意志を確認する（ステップＳ２２８）。

ユーザが所定の入力装置を介して料金を支払う旨を指示した場合は、支払い指示部４０３ｆに対し、支払い指示の発行を要求する（ステップＳ２２９～ステップＳ２３０）。支払い指示部４０３ｆで生成される支払い指示は、電子決済部４０６を経由してから所定のネットワークを介して電子決済業者のサーバ４０８に送信されるようになっている（ステップＳ２３１）。

【０１２８】

さて、電子決済業者のサーバ４０８で、料金の支払いが確認されると、その旨をライセン

ス情報更新サーバ４０７に通知するので、その通知を受けて、ライセンス情報更新サーバ４０７では、例えば、当該課金対象情報の利用期限を延長して新たなライセンス情報を生成し、それを暗号化して第２の情報再生装置へ送信する。第２の情報再生装置では、ネットワーク接続部４０５で更新されたライセンス情報を受信すると、ライセンス情報更新クライアント部４０３のライセンス情報入力部４０３ｇに入力され、さらに、ライセンス情報更新部４０３ｈに転送される（ステップＳ２３２～ステップＳ２３３）。ライセンス情報更新部４０３ｈは、受け取ったライセンス情報を情報蓄積部４０１に既に記録されている当該課金対象情報のライセンス情報に上書きすることによりライセンス情報を更新する（ステップＳ２３４）。

【０１２９】

次に、ライセンス情報更新サーバ４０７の構成および動作について、図３１および図３２を参照して説明する。図３０のステップＳ２２３で、第２の情報再生装置から送信されるライセンス情報は、ライセンス情報更新サーバ４０７のネットワーク接続部４０７ａで受信されると、ライセンス情報更新ユニット４０７ｂに転送される（図３２のステップＳ２４１～ステップＳ２４２）。ここで、必要があればライセンス情報を復号し、その復号されたライセンス情報は、ライセンス情報データベース４０７ｃに登録される（ステップＳ２４３）。このとき、ライセンス情報データベース４０７ｃでは、ライセンス情報の更新履歴を管理するため、登録の際にライセンス情報にフィールドＩＤを添付するようになっている。このフィールドＩＤは、ライセンス情報更新ユニット４０７ｂにも通知される。課金データベース（ＤＢ）検索部４０７ｄは、ライセンス情報に含まれる課金対象情報ＩＤをもとに課金データベース４０７ｅを検索し、支払い要求を生成する（ステップＳ２４４～ステップＳ２４６）。

【０１３０】

支払い要求の内容は、例えば、図３３に示すように、課金対象情報ＩＤ、その課金対象情報を利用するにあたり支払うべき料金の提示（利用期限と対応する料金）、料金の支払い先等が記述されている。

【０１３１】

生成された支払い要求は、フィールドＩＤとともに暗号化部４０７ｆに転送されて、暗号化された後、ネットワーク接続部４０７ａに転送され、ネットワークを介して第２の情報再生装置に送信されるようになっている（ステップＳ２４７～ステップＳ２５０）。暗号化された支払い要求とフィールドＩＤは、第２の情報再生装置で受信され、図３０のステップＳ２２４以降で説明したような処理される。

【０１３２】

さて、第２の情報再生装置では、図３０のステップＳ２３１で当該課金対象情報の利用に対する支払いを支払い指示を発行することにより行うが、その際の支払い指示の内容を、ユーザに提示された支払い要求が図３３に示したものであるとき、例えば、「１０円/１週間　for ”ＡＢＣＤ”to ａｂｃ、整理番号：フィールドＩＤ」と記述して、電子決済部４０６を通じて支払いを行う。ここで、整理番号は、ライセンス情報に付されたフィールドＩＤである。この支払い指示を受け取った電子決済業者のサーバ４０８は支払い処理を行った後、「１０円/１週間 for ”ＡＢＣＤ” from Ａ to ａｂｃ、整理番号：フィールドＩＤ」と言う明細を添えて、ライセンス情報更新サーバ４０７に支払い確認を送る。ここで、Ａはユーザのｉｄであるとする。

【０１３３】

ネットワーク接続部４０７ｇを介して支払い確認を受け取ったライセンス情報更新サーバ４０７では、まず、ライセンス情報更新ユニット４０７ｂにて、整理番号、すなわち、フィールドＩＤに基づいて、ライセンス情報データベース４０７ｃから更新すべきライセンス情報を検索する（ステップＳ２５１～ステップＳ２５３）。ライセンス情報更新ユニット４０７ｂは、さらに、支払い確認を参照して、ライセンス情報中の利用条件を更新し、再び暗号化して（ステップＳ２５４）、その暗号化したライセンス情報をネットワーク接続部４０７ａを介して第２の情報再生装置に送信する（ステップＳ２５５～ステップＳ２

５６）。
【０１３４】
ライセンス情報更新サーバから第２の情報再生装置に送信する支払い要求を暗号化するのは、次の理由による。すなわち、支払い要求を送信する通信路はインターネット等の公衆回線であって、一般にセキュリティが保証されていない。従って、例えば、支払い要求が改竄され、ユーザが不正な支払先に支払いを行う危険性が存在する。暗号化によって、それを防止する。
【０１３５】
図３４は、図２６に示した第２の情報再生装置を含むシステム全体の動作を概略的に説明するためのフローチャートである。なお、図３４に示した符号（ステップＳ２６１～ステップＳ２８６は、図２６に示した符号に一致し、その詳細な動作説明は前述した通りであるので省略する。
（３）ライセンス情報更新ユニット
次に、ライセンス情報更新ユニットについて説明する。ライセンス情報更新ユニットは、ライセンス情報の主に利用条件を更新するためのもので、例えば、前述の第１の情報記録装置により情報蓄積部に課金対象情報とともに記録されたライセンス情報の更新を行い、ライセンス情報更新ユニットを単体で利用することもできる。ライセンス情報を更新するために、ライセンス情報更新ユニットは、ライセンス情報に施されている暗号化を解除（復号）し、そこに別途入力された希望利用条件を入力し、その利用条件に対する支払いが行なわれたかを確認した後、それを暗号化し、更新されたライセンス情報として出力する必要がある。
【０１３６】
図３５にライセンス情報更新ユニットの構成例を示し、以下、図３６～図３７に示すフローチャートを参照して、図３５のライセンス情報更新ユニットの構成および動作を説明する。
【０１３７】
ライセンス情報更新処理に当たっては、まず、ライセンス情報入力部５０１へライセンス情報、希望利用条件入力部５０６へ希望利用条件が入力される（図３６のステップＳ３０１、図３７のステップＳ３０８）。ここでいうライセンス情報は、第１の情報記録装置で説明した利用条件と暗号化された課金対象情報の復号鍵ｋｄ（１）から構成されている。また、希望利用条件はユーザが希望する利用条件のことで、ユーザ側から適切なインターフェースを通して入力されるものとする。
【０１３８】
ライセンス情報入力部５０１に入力したライセンス情報は、復号鍵保持部５０３に保持されている復号鍵を用いてライセンス情報復号部５０２で復号され（図３６のステップＳ３０２）、利用条件と課金情報復号鍵を分離し、ライセンス情報（特に利用条件）を更新可能な状態にするとともに、課金対象情報ＩＤ等の課金に必要な情報を支払要求出力部５０７に送る（図３６のステップＳ３０３、図３７のステップＳ３１０）。更に更新可能な状態になったライセンス情報をライセンス情報更新部５０５で希望利用条件入力部５０６で入力された利用条件に書き換える（図３６のステップＳ３０４）。一方、希望利用条件に対する課金を行なうため、希望利用条件入力部５０６では入力された希望利用条件に対する課金を促すため、支払要求出力部５０７に希望利用条件の出力を行なう。支払要求出力部５０７では、希望利用条件入力部５０６から入力された希望利用条件とライセンス情報復号部５０２から入力された課金対象情報ＩＤ等の課金に必要な情報を予め定められた一定のプロトコルで装置外部に出力する（図３７のステップＳ３１０）。この出力に基づき外部装置では課金の具体的な手続きに入る。また、ここで出力される支払い要求情報はライセンス情報更新ユニットが組み込まれる著作権保護・課金のための情報流通システム（すなわち、本発明の情報記録装置、情報再生装置から構成される情報流通システム）の利用環境によって決まり、課金対象情報の著作権者が特定されている状況では課金対象情報ＩＤの出力は不要になるし、また、全課金対象情報について利用条件が予め定められてい

る場合には希望利用条件入力部５０６の存在や支払い要求出力部５０７からの利用条件の出力も不要になる。このように本実施形態のライセンス情報更新ユニットはそれが利用される環境により、いくつかの自明なバリエーションがあり得る。

【０１３９】

次に、支払要求情報に対する料金の支払いが完了した段階で、外部装置から支払い確認部５０８に支払い確認の信号が送られ、この信号が送られた時点で、ライセンス情報更新部５０５から入力された更新ライセンス情報を更新ライセンス情報暗号化部５０９に送り、暗号鍵保持部５１０に保持されている予め定められた暗号化鍵で暗号化する（図３６のステップＳ３０５、ステップＳ３０６）。この時、前記信号がくるまで更新されたライセンス情報は更新ライセンス情報暗号化部５０９へは送られない。この機能により本実施形態のライセンス情報更新ユニットは支払いが行なわれないにも関わらず更新ライセンス情報が出力されるのを防いでいる。

【０１４０】

更新ライセンス情報暗号化部５０９で暗号化された更新ライセンス情報は、更新ライセンス情報出力部５１１に送られ、外部装置に出力される（ステップＳ３０７）。ここで課金対象情報ＩＤとは、課金対象情報のＩＤであって当該情報の著作者を示し、課金額もしくは被課金者を特定するのに必要な情報である。

【０１４１】

なお、図３５に示したライセンス情報更新ユニットは、前述の第１の情報記録装置にて記録媒体等に記録されたライセンス情報の更新みならず、その変形例である第２、第３の情報記録装置にて記録媒体等に記録されたライセンス情報を更新する際にも適用できる。

【０１４２】

さらに、図３５に示したライセンス情報更新ユニットは、単体として用いることも、本発明の情報再生装置と組み合わせて、あるいは情報再生装置内に内蔵して用いることもできる。また、図３１のライセンス情報更新サーバのライセンス情報更新ユニット４０７ｂとして用いることもできる。

（４）著作権保護のための課金装置

図３８は、前述の情報記録装置にて記録媒体等に記録されたライセンス情報に基づき著作権保護のための課金を行う課金装置の要部の構成例を示したものである。

【０１４３】

図３８において、まず、磁気ディスクやＤＶＤディスク及びコンパクトディスクなどの記録媒体６１５からライセンス情報読み込み部６０１でライセンス情報を読み込み、それと同時にキーボートやマウスなどの入力媒体６１６を介して希望利用条件入力部６０２から希望利用条件を入力する。ライセンス情報及び希望利用条件はライセンス情報更新ユニット６０３に入力され、前述のライセンス情報更新ユニットの場合と同様なライセンス情報更新処理を経て、支払要求としての課金情報を課金情報検索部６０４に送る。ここで課金情報とは希望利用条件及び被課金者を特定するのに必要な情報である。課金情報検索部６０４では、これらの課金情報を基に課金情報データベース６０９を用いて課金額情報を検索する。また、課金額が予め定まっているような場合は、ライセンス情報更新ユニット６０３から敢えて希望利用条件を出力することをせず、課金額そのものを出力することもできる。この場合課金情報検索の必要はなくなる。更に課金対象情報の著作権者が特定されている場合はライセンス情報更新ユニット６０３から課金対象情報ＩＤ等の課金情報を出力する必要もなくなる。この場合後に述べる課金履歴管理部６０８では課金額情報のみを管理すればよく、課金対象情報ＩＤを管理する必要はなくなる。このようにライセンス情報更新ユニット６０３から出力される課金情報は本課金装置が応用される状況により、自明な変形がありうる。

【０１４４】

次に、課金情報および課金額情報は課金額情報出力部６０５に送られ、ユーザに課金額が提示される。ユーザが提示された課金額を何らかの方法で支払うと、続く支払い判定部６０６で支払いの確認が行なわれ、支払いが行なわれた旨の信号が前述のライセンス情報更

新ユニットの支払い確認部５０８に送られる。ここで述べているユーザの課金額支払いの方法は現金支払いによる場合は紙幣・硬貨挿入部とそれらの判定部を有し、この判定部の判定に応じて支払い判定部６０６に信号を送る。また、支払いは電子マネーである場合やクレジットカードもしくはプリペイドカードである場合など様々であり、各々に独自の判定の仕方が存在する。

【０１４５】

支払い判定部６０６で支払い完了の判定がでたら、支払い判定部６０６は課金履歴管理部６０８に課金情報を送りそれらを保存管理する。

【０１４６】

本実施形態の課金装置は、外部とネットワーク等で接続されていないことを前提としているので課金決済はその場では完了しない。故に本実施形態はこのような支払いをどのように分配するかを管理する必要があり、課金履歴管理部６０８が必要となる。ここに蓄積された履歴情報は定期的に一定の管理者によって読み取られ、しかるべき手段で決済される。

【０１４７】

最後に、支払い判定部６０６からの支払済みの信号を受けたライセンス情報更新ユニット６０３は、前述のライセンス情報更新ユニットと同様な手続きを経て更新ライセンス情報を更新ライセンス情報書き込み部６０７に出力し、書き込み部６０７は更新ライセンス情報を入力記録媒体６１５の適切な箇所に書き込む。本実施形態の課金装置を本発明の情報再生装置と組み合わせれば、いわばライセンス情報の更新機能を持った著作権のある情報の自動販売機のようなものを構成できる。すなわち、本発明の特徴的な機能が１つの匡体の中で実現されるところに特徴がある。このように構成することにより、著作権のある課金対象情報をレンタルもしくは販売する場合、持ち運び可能なＤＶＤやＣＤその他の記録媒体に（暗号化された）課金対象情報が既に入力されているという仮定のもとで、その記録媒体を本実施形態の課金装置に入力することで適切な課金処理を行なうことができ、いつでも誰でも手軽にコンテンツの利用権を買うことができる。

（４－１）課金対象情報の不正コピーの防止対策を講じたライセンス情報更新ユニットおよびそれに対応する情報再生装置の復号ユニット

容易に分かるように、コピーライトのある課金対象情報に永久利用を認めたり、非常に長い利用期限を認めたりすると、その記憶媒体そのものが複製される危険があり、もし複製品が大量に出回ったら、コピーライトは保護できなくなる。このことを解決するために、本実施形態の復号ユニットおよびライセンス情報更新ユニットは、利用条件として永久利用あるいは非常に長い利用期限を許可する場合、手持ちのただ１つの復号ユニットのみに課金対象情報の再生を限定しようとするものである。なお、以下の説明において、利用条件として「無期限」あるいは「永久利用」とあるのは、永久利用あるいは非常に長い利用期限を許可する場合を含むものとする（後述（４－２）の説明およびその他の説明においても同じ）。このようにすれば違う復号ユニットを使って利用しようとしても利用拒否することができ、例え複製してもあまり利益がなくるので、逆にコピーライトが保護される。しかし、この場合、課金対象情報永久利用権購入時に復号ユニットＩＤ（復号ユニットを特定するＩＤ）が分からないと購入できないことになってしまう。このため、本実施形態のライセンス情報更新ユニットは永久利用権購入コンテンツを最初に利用する時に利用条件に復号ユニットＩＤを付加することを特徴としている。なお、復号ユニットＩＤは、各復号ユニットのそれぞれを識別するための識別情報であり、例えば、各復号ユニットの製造番号であってもよい。

【０１４８】

図３９は、本実施形態の復号ユニットの構成例を示したものである。以下、図４０に示すフローチャートを参照して復号ユニット７０１の構成および動作について説明する。

【０１４９】

ライセンス情報がライセンス情報入力部７１１から入力されると（ステップＳ４０１）、それが復号部７１２へ送られ、復号部７１２では、復号鍵保持部７１３に保持された復号

鍵でライセンス情報を復号する（ステップＳ４０２）。復号されたライセンス情報は利用条件変更必要性判定部７１４に送られる（ステップＳ４０３）。利用条件変更必要性判定部７１４では、利用条件中の利用期限が無制限である場合、それが特定の復号ユニットＩＤに限定されているか否かを判定し、限定されいない場合、利用条件変更の必要ありと認め、その更新をライセンス情報更新ユニット７０２に委ねるようになっている。すなわち、利用条件変更必要性判定部７１４では送られた復号されたライセンス情報から利用条件を読み込み利用期間が無制限か否かの判定を行なう（ステップＳ４０４）。無制限であったら利用条件が復号ユニットＩＤに限定されているか否かを判定し（ステップＳ４０５）、限定されていれば、判定部７１５に利用条件を送り、判定部７１５では復号ユニットＩＤ参照部７１６に復号ユニットＩＤの提示の指示を送り（ステップＳ４０６）、同参照部７１６から提示された復号ユニットＩＤと利用条件に記載されていた復号ユニットＩＤを比較し（ステップＳ４０７）、一致した場合、暗号化された課金対象情報（コンテンツ）の復号鍵ｋｄ（１）を出力して終了し（ステップＳ４０８）、一致しない場合たとえばＮＵＬＬコード（通常は０）を出力して復号出来ない旨の指示とし、終了する（ステップＳ４０９）。また、利用条件が無期限で復号ユニットＩＤが記載されていない場合、利用条件変更必要性判定部７１４は利用条件に復号ユニットＩＤを記載する必要を認め、復号ユニットＩＤ参照部７１６から復号ユニットＩＤを取得し、その取得した復号ユニットＩＤと暗号化されたライセンス情報とをライセンス情報更新ユニット７０２に送る（ステップＳ４１０）。

【０１５０】

さらに、利用条件が無期限でない場合は（ステップＳ４０４）、利用条件を判定部７１５に送り、判定部７１５では時計参照部７１７から現在時刻の提示を受け（ステップＳ４１１）、その時刻から利用の可否を判定し、可の場合は暗号化された課金対象情報（コンテンツ）の復号鍵ｋｄ（１）を出力し終了し（ステップＳ４１２～ステップＳ４１３）、否の場合は前述同様ＮＵＬＬコードを出力し終了する（ステップＳ４１４）。

【０１５１】

図４１は、ライセンス情報更新ユニット７０２の構成例を示したものである。以下、図４２に示すフローチャートを参照しながら、図４１のライセンス情報更新ユニット７０２の構成および動作について説明する。

【０１５２】

ライセンス情報更新ユニット７０２は、ライセンス情報入力部７２１に入力されたライセンス情報をライセンス情報復号部７２３に送り、ライセンス情報復号部７２３でその情報を復号鍵保持部７２４からの復号鍵を基に復号する（ステップＳ４２１～ステップＳ４２２）。復号されたライセンス情報はライセンス情報更新部７２５に送られ、そこから利用条件が抽出される（ステップＳ４２３）。一方、復号ユニットＩＤ入力部７２２に入力した復号ユニットＩＤは、ライセンス情報更新部７２５に送られ（ステップＳ４２４）、ライセンス情報更新部７２５では、先に抽出された利用条件に復号ユニットＩＤの限定を付加し、利用条件を更新する（ステップＳ４２５）。さらに、この更新された利用条件を基に新たなライセンス情報を生成し、それを更新ライセンス情報暗号化部７２６に送る。更新ライセンス情報暗号化部７２６では、暗号鍵保持部７２７から提示された暗号鍵を基に更新されたライセンス情報を暗号化した後（ステップＳ４２６）、更新ライセンス情報出力部７２８に送り、ライセンス情報更新ユニット外部７０２外部に送り出す（ステップＳ４２７）。

【０１５３】

なお、ライセンス情報更新ユニット７０２と復号ユニット７０１とを一体化させ、１つのユニットとし、例えば、図３８の情報流通システムのライセンス情報更新ユニット６０３に置き換えることも可能である。

（４－２）課金対象情報の不正コピーの防止対策を講じた復号ユニットの他の例

前述の（４－１）で述べたように、永久利用権あるいは非常に長い利用期限が認められている（以下、この２つの場合を永久利用権の範疇に含めるものとする）課金対象情報は複

製されることによってコピーライトが保護できない状態になる可能性がある。この問題は前述の（４－１）で述べたライセンス情報更新ユニットおよびそれに対応した復号ユニットを用いることにより、ほぼ解決している。即ち、永久利用権の認められている課金対象情報の利用を１つの復号ユニットＩＤに限定しようとするものであった。この場合問題になるのは永久利用権購入時に購入者が持つ復号ユニットＩＤが分からないことがあり得るという点であった。そこで、次に示す第２の復号ユニットでは、永久利用権を取得した課金対象情報を最初に利用する場合、永久利用の旨を記載するところに利用する復号ユニットＩＤを書き込み、以後その復号ユニットＩＤでしか復号できないようにした。

【０１５４】

しかしながら、この方式の場合、最初に利用する前に複製される危険があり、ここで複製された永久利用権のある課金対象情報が大量に流布すればやはりコピーライトは保護できなくなる。そこで、第２の復号ユニットでは、永久利用の利用条件にメディアＩＤを含め、利用時にこれを参照することを特徴としている。ここでメディアＩＤとは、ＤＶＤやＣＤディスクであればその製造番号であり、一般に、後から改変出来ないＲＯＭ領域に書かれていることを前提としている。この利用条件が特定のメディアＩＤに限定されていることから他のメディアに複製されても複製側のメディアＩＤがオリジナルのメディアＩＤと異なるため利用条件に合わず利用できないことになる。

【０１５５】

図４３は、第２の復号ユニットの構成例を示したものである。以下、図４４に示すフローチャートを参照して図４３の第２の復号ユニットの構成および動作について説明する。

【０１５６】

ライセンス情報は、ライセンス情報入力部７４１に入力され、復号部７４２に送られる（ステップＳ４３１）。復号部７４２では、復号鍵保持部７４３に保持されている復号鍵を用いてライセンス情報の復号を行ない、利用条件とその他のものとを分離する（ステップＳ４３２）。分離された利用条件は利用条件変更必要性判定部７４４に送られ、ここで利用条件に復号ユニットＩＤの限定を入れるか否かを判定する。すなわち、前述の（４－１）でも詳しく述べたように利用期限が無期限で、かつ、復号ユニットＩＤが特定の復号ユニットに限定されていない利用条件には復号ユニットＩＤの限定を入れなければならず、この場合のみ利用条件変更の必要があると解釈され、復号ユニットＩＤ参照部７４６から復号ユニットＩＤを取得し、抽出されたライセンス情報と共にライセンス情報更新ユニット７３２に送る（ステップＳ４３４、ステップＳ４３５、ステップＳ４４７）。その他の場合は利用条件情報を判定部７４５に送り、利用条件の判定を行なう。

【０１５７】

判定部７４５では次のような処理を行ない、利用条件が有効なものか否かを判定する。まず、利用条件が無期限であって、復号ユニットＩＤに限定されている場合、利用条件にメディアＩＤの限定があるか否かを判定し、ある場合にはメディアＩＤ保持部７４８に保持された当該課金対象情報が入っているメディアのメディアＩＤを参照し、それと利用条件の限定となっているメディアＩＤとの比較を行ない、一致していれば復号鍵ｋｄ（１）を出力し終了する（ステップＳ４３４～ステップＳ４４０）。一致していなければ利用拒否の旨の信号、この場合はＮＵＬＬを出力し処理を終了する（ステップＳ４４１）。メディアＩＤの限定がない場合には（ステップＳ４３８）、復号鍵ｋｄ（１）を出力し終了する（ステップＳ４４２）。なお、ここで参照されるメディアＩＤはメディアＩＤ入力部７４７からのメディアＩＤの入力を受けメディアＩＤ保持部７４８に保持されている。

【０１５８】

一方、利用条件が有期限の場合（ステップＳ４３４）、まず、時計参照部７４９を介して現在の時刻を参照し（ステップＳ４４４）、その時刻が期限内かどうかを判定する（ステップＳ４４５）。期限内でない場合、利用拒否の旨の信号、この場合はＮＵＬＬを出力し終了する（ステップＳ４４６）。期限内である場合は、ステップＳ４３８に進み、利用条件にメディアＩＤの限定があるか否かを判定し、以降、無期限の場合と同様のアルゴリズムで利用条件の有効性を判定し、その結果によってそれぞれ出力し終了する。

【０１５９】
なお、メディアＩＤの趣旨から有期限の場合の利用条件にはメディアＩＤの限定は必要ないように思われるかもしれないが、有期限といっても期間が長い場合もあり、このような場合はその期間内はコピーライトを十分には保護できない。更に例え期間内であっても無闇に複製されては不都合となる課金対象情報もあり、この場合にも第２の復号ユニットは有効である。
【０１６０】
同様のことは、復号ユニットＩＤに関しても言えるので、有期限の利用条件であっても利用条件の復号ユニットＩＤの限定は有効であり、その実現は前述のメディアＩＤの限定の場合と同様である。また、このことは、前述の（４－１）についても同様である。
（５）コピー装置
図４５に、例えば、図１の第１の情報記録装置にて記録媒体等に記録された情報のコピーを行うコピー装置の構成例を示す。以下、図４６に示すフローチャートを参照して図４５のコピー装置の構成および動作について説明する。
【０１６１】
コピーの基本的な考え方は、情報コピーの際の利用条件のデフォルト化である。すなわち、あるメディア（図４５のメディア８０１）に記録されている課金対象情報のライセンス情報は、有効な利用条件を含んでいるかも知れないが、図４５のコピー装置では、その複製を作成する際に、この利用条件を消去して、他のメディア（図４５のメディア８０２）に記録するようになっている。
【０１６２】
まず、コピー元のメディア８０１に記録されている１単位の情報（例えば、暗号化された課金対象情報とそのライセンス情報）を読み出し部８０３で読み出し（ステップＳ５０１）、ライセンス情報のみをライセンス情報複製ユニット８０４へ転送する（ステップＳ５０２）。一方、読み出し部８０７は、コピー先のメディア８０２のメディアＩＤを読みとり、それをライセンス情報複製ユニット８０４に転送する（ステップＳ５０３～ステップＳ６０４）。ライセンス情報複製ユニット８０４は、コピー元のメディア８０１から読み出されたライセンス情報をデフォルト化し、コピー先のメディア８０２のメディアＩＤを利用条件に書き込むことにより、ライセンス情報を更新し（ステップＳ５０５）、その更新されたライセンス情報を書き込む部８０６に出力する（ステップＳ５０６）。
【０１６３】
ライセンス情報複製ユニット８０４は、例えば、図４７に示すような構成である。以下、図４８に示すフローチャートを参照してライセンス情報複製ユニット８０４の構成および動作についても説明する。
【０１６４】
ライセンス情報がライセンス情報複製ユニット８０４のライセンス情報入力部８１１に入力すると（図４８のステップＳ５１１）、復号部８１２に転送され（ステップＳ５１２）、ここで復号される（ステップＳ５１３）。復号されたライセンス情報はライセンス情報更新部８１３に転送される（ステップＳ５１４）。一方、コピー先のメディア８０２のメディアＩＤはメディアＩＤ入力部８１４に入力され（ステップＳ５１５）、ライセンス情報更新部８１３に転送される（ステップＳ５１６）。ライセンス情報更新部８１３は、コピー元のメディア８０１から読み出されたライセンス情報の利用条件をデフォルト化し、さらに、コピー先のメディア８０２のメディアＩＤを利用条件に書き込み、ライセンス情報を更新する（ステップＳ５１７～ステップＳ５１８）。この更新されたライセンス情報はライセンス情報出力部８１５に転送されて（ステップＳ５１９）、図４５の書き込み部８０６に出力される（ステップＳ５２０）。
【０１６５】
図４５の説明に戻り、書き込み部８０６は、更新されたライセンス情報をコピー先のメディア８０２に書き込むとともに、読み出し部８０３から転送されてきた課金対象情報を同じくメディア８０２に書き込み、コピー処理を終了する（図４６のステップＳ５０７～ス

テップＳ５０９）。

【０１６６】

このように、図４５のコピー装置では、ライセンス情報複製ユニット８０４でコピー元のメディア８０１から読みとったライセンス情報の利用条件を消去するため、コピー先のメディア８０２に記録されている課金対象情報は、メディア８０１のそれと同一でありながら、ライセンス情報に有効な利用条件を含まないようになっている。従って、メディア８０２に記録されている情報を、例えば、図４３に示したような復号ユニットを具備する情報再生装置で再生しようとしても、その利用が拒絶される。すなわち、ライセンス情報の復号が可能であるのは復号鍵を有する復号ユニットのみであり、課金対象情報の暗号化を解除する為にはライセンス情報に含まれる課金対象情報用の復号鍵が必要であるから、結局、当該課金対象情報は、そのままでは、利用不可能である。メディア８０２に複製された課金対象情報を利用する為には、何らかの正当な課金手続きを経て、有効な利用条件をライセンス情報に添付しなければならないことになる。

【０１６７】

なお、利用条件のデフォルト化は、有効な利用条件の消去に限るものではない。例えば、コピー後一日だけ有効とする利用条件を記入する事も可能である。すなわち、例えば、現在が４月１６日の１３：００であるとすれば、４月１７日の２３：５９を利用期限とする利用条件を記入する。

【０１６８】

さらに、図４５のコピー装置は、利用条件をデフォルト化するとともに、コピー先のメディア８０２のメディアＩＤの書き込みを行うが、メディアＩＤは、課金対象情報が記録されているメディアを特定する文字列であり、例えば、ＤＶＤ－ＲＡＭのＲＯＭ領域に記入されている製造番号である。あるいは、ハードディスク装置の製造番号であってもよい。

【０１６９】

本実施形態では、メディアＩＤはライセンス情報に含まれている。メディアＩＤを利用する復号ユニットは、ライセンス情報復号時にメディアＩＤの確認を行い、再生しようとしている情報の記録されているＤＶＤ－ＲＡＭのメディアＩＤが、ライセンス情報に含まれているメディアＩＤに一致しない場合、前述したように、課金対象情報復号用の復号鍵を出力しないようになっている。復号ユニットが、この様な動作を行う事は、課金対象情報自身が、その「入れ物」を指定する効果を生じさせる。

【０１７０】

ライセンス情報がメディアＩＤを含む課金対象情報は、本実施形態に述べる様な、正統な（i.e.復号鍵を有する）コピー装置によってのみ、コピー可能である。コピー先のメディア８０２をメディアＩＤの確認を行う復号ユニットを備えた情報再生装置によって再生可能とする為には、メディア８０２のメディアＩＤをライセンス情報の利用条件中に埋め込む必要がある。図４５のコピー装置は、この処理を行っている。

（６）情報再生装置の第３の例：副情報（広告や著作権の利用に関する警告等）の視聴に復号ユニットを利用する情報再生装置

図４９は、第３の情報再生装置の構成例を示したものである。本発明の情報記録装置により記録媒体等に記録された情報に含まれる副情報（広告や著作権の利用に関する警告等）の視聴の確実を期するため、副情報の中に視聴確認データがちりばめられている。例えば、副情報中の少なくとも２カ所以上に視聴確認データがちりばめられている。副情報の一例を以下に示す。

【０１７１】

「始０Ｔｈ０めに、ロゴスはおられた。０ｉｓ０ロゴスは神とともにおられ００た。ロ０ｉｓ０ゴスは０ｔｈ０神であった。この方は始めに神と０ｅ　ｃ０ともにおられた。一切のもの０ｅｒｔｉ０はこの方によってできた０ｆｉ０。できたもので０ｃａｔ０この方によら０ｉｏｎ０ずにでき０ｄａ０たものは、ただの一つも０ｔａ．０な００い。」

図４９の視聴確認データ抽出部９０３では、入力された副情報を再生部９０５に送り再生すると同時に、その副情報を順に調べ、２つの「０」で囲まれた文字を取り出していく。

２つの「０」の間が空であれば、取り出した文字列を格納する。上記の例では、「ｔｈｉｓ ｉｓ ｔｈｅ ｃｅｒｔｉｆｉｃａｔｉｏｎ ｄａｔａ．」という文字列が視聴確認データとして抽出され、視聴確認データ抽出部９０３に具備される所定のメモリに格納されることになる。このように、副情報中の少なくとも２カ所以上に視聴確認情報をちりばめることがポイントである。副情報中に視聴確認情報をちりばめることにより、副情報を全て再生しない限り、視聴確認データを再生することができない。従って、視聴確認データをもって、視聴の確認と見なすことができる。

【０１７２】

以下、図５０に示すフローチャートを参照して、図４９の第３の情報再生装置の構成および動作について説明する。

【０１７３】

情報蓄積部９０１は、図８の第１の情報再生装置の情報蓄積部１０１と同様である。情報蓄積部９０１から、情報読み出し部９０２にて読み出された１単位の情報には、暗号化された課金対象情報とそのライセンス情報と副情報が含まれている。そのうち、暗号化された課金対象情報を再生部９０５に転送し（ステップＳ６０１）、副情報を視聴確認データ抽出部９０３へ転送する（ステップＳ６０２）。視聴確認データ抽出部９０３では、副情報を走査して視聴確認データを抽出する（ステップＳ６０３）。読み出し部９０２は、ライセンス情報を復号ユニット９０４へ転送する（ステップＳ６０４）。

【０１７４】

ライセンス情報の利用条件中には、当該課金対象情報の再生条件として視聴確認データが含まれている。復号ユニット９０４は、視聴確認データ抽出部９０３が確認している視聴確認データを読み出し、照合を行う（ステップＳ６０５～ステップＳ６０６）。視聴確認データが求めるものに一致していれば、続く処理を行う（ステップＳ６０７）。すなわち、利用期限等他の利用条件の確認を行った後、課金対象情報の復号用の鍵を再生部９０５に出力し、課金対象情報の再生を行う（ステップＳ６０８～ステップＳ６１１）。

【０１７５】

図５１は、復号ユニット９０４の構成例を示したものである。以下、図５２に示すフローチャートを参照して復号ユニット９０４の構成および動作について説明する。

【０１７６】

復号ユニット９０４に転送されたライセンス情報は、ライセンス情報入力部９０４ａに入力し（ステップＳ６２１）、復号部９０４ｂに転送される（ステップＳ６２２）。復号部９０４ｂでは、復号鍵保持部９０４ｃに保持されている復号鍵ｋｄを用いてライセンス情報を復号した後、視聴確認部９０４ｄに転送する（ステップＳ６２３～ステップＳ６２５）。一方、視聴確認データ抽出部９０３から送られてきた視聴確認データは、視聴確認データ入力部９０４ｅに入力され、視聴確認部９０４ｄに転送される（ステップＳ６２６）。視聴確認部９０４ｄでは、ライセンス情報の利用条件中に含まれる当該課金対象情報の再生条件としての視聴確認データと、視聴確認データ抽出部９０３から送られてきた視聴確認データとを照合し（ステップＳ６２７）、これらが一致しているとき、ライセンス情報を判定部９０４ｆに転送する（ステップＳ６２８～ステップＳ６２９）。判定部９０４ｆでは、ライセンス情報中の利用条件に基づき課金対象情報の利用の可否（すなわち、復号鍵ｋｄ（１）を再生部９０５に出力するか否か）を判定して、その判定結果に応じて、復号鍵を再生部９０５に出力する（ステップＳ６３０～ステップＳ６３２）。

（追記）

以上説明した本発明の情報記録装置では、１つの課金対象情報に対し１つのライセンス情報を対応させて記録媒体等に記録する場合に限らず、１つの課金対象情報に対し、複数のライセンス情報を対応させて記録媒体等に記録するようにしてもよい。

【０１７７】

また、本発明の情報再生装置では、課金対象情報の利用の可否を判定する場合、該課金対象情報に対応する１つのライセンス情報に含まれる利用条件を参照するようになっているが、この場合に限らず、記録媒体に１つの課金対象情報に対応して複数のライセンス情報

が記録されている場合には、これら全てのライセンス情報に含まれる利用条件を順次参照して該課金対象情報の利用の可否を判断するようにしてもよい。すなわち、複数のライセンス情報のそれぞれに含まれる利用条件のうち、条件を満たすものが１つでもあれれば、該課金対象情報の利用を可能と判断する。

【０１７８】

また、本発明の情報再生装置および課金装置において、ライセンス情報を更新する際には、既に記録媒体に記録されているライセンス情報を書き換える場合に限らず、該記録媒体に追加記録することも可能である。従って、上記実施形態の記録媒体等に記録されたライセンス情報の更新に関する説明中、「更新」は、「上書き記録」と「追加記録」を含むものである。

【０１７９】

さらに、利用条件に含まれる復号ユニットＩＤ、メディアＩＤ等は、必ずしも１つである必要はない。

（第２の実施形態）

（１）　復号ユニットＡ

図５４は、第２の実施形態に係る復号判定装置、すなわち、復号ユニットＡの構成例を示したものである。

【０１８０】

復号ユニットＡは、主にデジタルコンテンツである有料データに付属するライセンス情報を基に当該コンテンツの利用が可能か否か（すなわち、例えば契約により定められた利用条件に基づく該コンテンツ情報の利用のライセンスが有効か無効か）のチェックを行い、有効ならば該コンテンツ情報を利用するためのコンテンツ復号鍵をビデオ再生装置などのコンテンツ情報の再生等を行うための情報利用装置に出力するものである。

【０１８１】

尚、ここではコンテンツ情報は予め暗号化されていて、その復号鍵（以下コンテンツ復号鍵という）を利用有効期限等のコンテンツ利用条件や当該コンテンツ情報の識別情報（ＩＤ）などとともにライセンス情報に入れ、当該ライセンス情報全体を暗号化して、暗号化されたコンテンツ情報とともに契約ユーザに提供する（例えば、放送配信、記録媒体に格納して配布等）。

【０１８２】

ライセンス情報の復号は復号ユニットＡ内に存在する秘密鍵で行う。図５５にライセンス情報の一例を示す。図５５に示すように、ライセンス情報には、少なくともコンテンツ復号鍵、当該コンテンツ情報の利用有効期限等のコンテンツ利用条件、当該コンテンツ情報のＩＤが含まれている。

【０１８３】

ライセンス情報を復号する秘密鍵が全ての復号ユニットに共通のものであると、運用上は便利ではあるが、ひとたびこの秘密鍵が外部に洩れればこの復号ユニットを使って復号されるライセンス情報に含まれるコンテンツ復号鍵が原理的に全て読み取れることになる。これはライセンスを保護することを目的とする復号ユニットＡとしては深刻な問題であり、これを解決するのが本発明の目的である。

【０１８４】

本実施形態の復号ユニットＡでは、この問題点を解決するため、ライセンス情報を復号するための秘密鍵を復号ユニットＡ内で生成し、これをある一定期間に限って用いるようになっている。

【０１８５】

次に、図５７に示すフローチャートを参照して、図５４の復号ユニットＡの各構成部の動作について説明する。

【０１８６】

暗号化されたライセンス情報は、ライセンス情報入力部２００１を通じて復号ユニットＡ内に入力され（ステップＳ１００１）、復号部２００２で復号された後（ステップＳ１０

０２）、判定部２００３に送られ、利用条件のチェックにより当該ライセンスが有効か否かが判定される（ステップＳ１００３～ステップＳ１００４）。ここで、ライセンスが有効か否かの判定とは、利用条件が満たされているか否か、すなわち、例えば、当該コンテンツの利用有効期限を経過していないか否かを判定するものとする。

【０１８７】

判定部２００３にて有効（コンテンツの利用可能）という判定が出ればライセンス情報に含まれるコンテンツ復号鍵を情報利用装置２０２０に出力する（ステップＳ１００５）。

【０１８８】

一方、無効（コンテンツの利用不可）という判定が出れば当該ライセンス情報を更新情報生成部２００４に送り、ライセンスの更新（すなわち、ライセンス情報の更新）に必要な情報をまとめ、ライセンス情報を更新するための更新情報を生成して、ライセンス情報更新装置２００８に例えば所定の通信回線（例えば、専用回線、インターネット等でもよい）を経由して出力する（ステップＳ１００６～ステップＳ１０１０）。

【０１８９】

更新情報生成部２００４は、利用条件入力部２００９を介して入力されたユーザの希望する利用条件（利用期限の延長等）と、判定部２００３から送られたライセンス情報とに基づき、少なくとも当該コンテンツのＩＤ、鍵生成部２００６で生成された復号ユニットＡの公開鍵を含む更新情報（図５６参照）を生成するようになっている。

【０１９０】

復号ユニットＡには、前述したように、暗号化されたライセンス情報を復号するための秘密鍵を生成する鍵生成部２００６を具備しいている。鍵生成部２００６では、ライセンス情報を暗号化／復号化するための鍵を生成する。鍵生成手法としては、例えば、公開鍵暗号の鍵生成のアルゴリズムを用いてもよく、ＲＳＡ暗号の場合は乱数と素数判定アルゴリズムを用いて適当な長さ（例えば、５１２ｂｉｔ程度）の２つの素数ｐ、ｑを生成する。

【０１９１】

ここで乱数のアルゴリズムは全ての復号ユニットＡで共通であっても、乱数の種の取り方に時間のマイクロ秒をとるなどの工夫をすれば同じ素数が生成される可能性は極めて低い。

【０１９２】

次に、Ｎ＝ｐ・ｑとしＮを求める。同時に、Ｍ＝（ｐ－１）（ｑ－１）を求め、

【０１９３】

【数１】

$$ed \equiv 1 \pmod{M}$$

となるような整数ｅ、ｄ（０＜ｅ、ｄ＜Ｍ）を求める。ｅ、ｄは、まず、ｄを決め、それに対応するｅをユーグリッドの互除法というアルゴリズムを用いて求めるようにすると比較的容易に求められる。この一方（例えばｅ）を秘密鍵、他方（例えばｄ）とＮを公開鍵とすれば、これらの鍵を使い、公知のＲＳＡ暗号のアルゴリズムによって公開鍵暗号が実現される。

【０１９４】

さらに、これらの鍵は当該復号ユニットＡに固有のものであり、これを当該ユニットの中から何らかの手段で読み出したとしても他のユニットでは利用できないし、一定期間を過

ぎれば無効になるように鍵保持部２００５でスケジューリングすれば同じユニットでも一定期間を過ぎれば利用できなくなる。なお、鍵生成部２００６は鍵保持部２００５によって駆動される。

【０１９５】

鍵保持部２００５は予め定められたタイミングで鍵生成部２００６に鍵生成の命令を送る。このタイミングは例えば図１の時計参照部２００７で参照した時刻を基にする方法が一般的である。

【０１９６】

図５８は、鍵保持部２００５、鍵生成部２００６における鍵生成処理の概略手順を説明するためのフローチャートである。鍵保持部２００５は、例えば、所定時間毎に時計参照部２００７を介して時刻を参照し（ステップＳ１０２１）、予め定められた鍵の更新時刻であるときは、鍵生成部２００６に対し鍵生成の命令を送り、鍵生成部２００６では前述したような公開鍵および秘密鍵の生成を行う（ステップＳ１０２２～ステップＳ１０２３）。現時刻が鍵更新時刻でないときは所定時間待つ（ステップＳ１０２５）。鍵生成部２００６で生成された公開鍵および秘密鍵は鍵保持部２００５に保持される（ステップＳ１０２４）。

【０１９７】

このように鍵生成部２００６にて鍵の何度も生成を行わなくとも、復号ユニットＡを最初に使うときに初期化動作として一回鍵生成を行うだけでも、異なる復号ユニットＡには異なる鍵が設定されることになり有効性は高い。もちろん、工場出荷時に別々の鍵を鍵保持部２００５にセットすることも考えられる。この場合は鍵生成部２００６は不要である。

【０１９８】

本発明の復号ユニットＡの特徴として、ライセンス情報を更新する際、鍵保持部２００５が保持している公開鍵をライセンス情報を更新するために必要な他の情報とともにライセンス情報更新装置２００８に送信する必要がある（この公開鍵は、ライセンス情報更新装置２００８にて新たに生成された更新されたライセンス情報を暗号化する際に用いられるからである）。この手続きを行うのが更新情報生成部２００４である。

【０１９９】

更新情報生成部２００４は、判定部２００３でライセンス情報に基づきコンテンツの利用が不可と判定されたとき起動され、利用条件入力部２００９を起動し、ユーザに対し、希望する利用条件（例えば、延長期間等）の入力を促す。これと並行して鍵保持部２００５に公開鍵の出力を促し、得られた公開鍵と希望利用条件を判定部２００３から送られるコンテンツＩＤなどの課金に必要な情報とともに予め定められたフォーマットに整理し、ライセンス情報を更新するための更新情報（図５６参照）として、ライセンス情報更新装置２００８に送る。

【０２００】

時計参照部２００７は内部（場合によっては外部）にある時計２０１０を参照し、鍵保持部２００５の鍵生成のタイミングを計るために用いるほか、利用条件の利用有効期限のチェックときにも用いられる。

（２）　復号ユニットＢ

図５９は、復号判定装置の他の構成例を示したものである。すなわち、復号ユニットＢの構成例を示したもので、復号ユニット内で（一時的にでも）コンテンツ復号鍵が未暗号化データとして存在する状態を解消することができる。

【０２０１】

コンテンツ復号鍵が当該ユニット内で未暗号化データとして存在すると当該ユニットを解析された際、読み取られる危険性が生ずる。もし恒常的に読み取ることができれば、その方法を使ってあらゆるコンテンツ復号鍵は（復号ユニットが有する秘密鍵を知らなくても）取得できることを意味し、ライセンス保護の観点から重大なセキュリティーホールとなる。この問題はその性質上秘密鍵を一定期間で生成し、古いものと置き換えるという前述の復号ユニットＡの方法では解決できない。

【０２０２】
復号ユニットＢ内では、コンテンツ復号鍵が暗号化されたままであり、当該復号ユニット内の情報だけでは暗号化されたコンテンツ復号鍵を復号できないような構成となっている。

【０２０３】
図６１に示すフローチャートを参照して、図５９の復号ユニットＢの各構成部の動作について説明する。

【０２０４】
暗号化されたライセンス情報はライセンス情報入力部２００１を通じて、復号ユニットＢに入力し、例えば、復号部２００２で復号ユニットＢ内に予め保持されている秘密鍵で復号される（ステップＳ１０３１～ステップＳ１０３２）。

【０２０５】
図６０は復号ユニットＢに入力されるライセンス情報の一例を示す。図６０に示すように、ライセンス情報には、少なくともコンテンツＩＤ、当該コンテンツの利用条件の他に、暗号化されたコンテンツ復号鍵［ｋｃ］K_{AB}と、この暗号化されたコンテンツ復号鍵を復号するための共有鍵生成情報ｋａとが含まれている。なお、コンテンツ復号鍵ｋｃは、共有鍵K_{AB}で暗号化されているものとする。
さて、復号部２００２で復号されたライセンス情報は、判定部２００３へ送られ、ここで利用条件の判定が行われる（ステップＳ１９３３）。利用条件が満たされれば、暗号化されたコンテンツ復号鍵［ｋｃ］K_{AB}と共有鍵生成情報ｋａとが情報利用装置２０２０へ送られる（ステップＳ１０３４～ステップＳ１０３５）。

【０２０６】
一方、判定部２０３で利用不可と判定された場合は、更新情報生成部２００４へライセンス更新に必要なコンテンツＩＤなどを送る（ステップＳ１０３４、ステップＳ１０３６）。

【０２０７】
更新情報生成部２００４は、共有鍵生成情報抽出部２０３１を介して当該コンテンツを利用する情報利用装置２０２０に対して、ライセンス情報更新装置２００８においてコンテンツ復号鍵を暗号化するために必要な共有鍵生成情報ｋｂの出力を促す。

【０２０８】
ここで、コンテンツ復号鍵を暗号化するための共有鍵生成情報ｋａ、ｋｂについて説明する。離散対数問題を安全性の根拠にした公開鍵暗号（例えば楕円曲線暗号）においては、以下のような共有鍵生成プロトコルが考えられる。まず情報利用装置２０２０とライセンス情報更新装置２００８に共通なｘという元を予め定めておく。さらに、情報利用装置２０２０内に（例えば出荷時に定めた）整数ｂとｘとｂから計算される元x^bとを予め求めて格納しておく。そしてライセンス更新の要求があった場合には、x^bを復号鍵生成情報ｋｂとして復号ユニットＢに送る。

【０２０９】
復号ユニットＢでは、利用条件入力部２００９を介してユーザから入力された希望利用条件の他に復号鍵生成情報ｋｂとコンテンツＩＤとを含む更新情報（図６２参照）を生成して、ライセンス情報更新装置２００８に送る。

【０２１０】
ライセンス情報更新装置２００８では、乱数等を使って自ら決めた整数ａを使って、復号ユニットＢから送られてきた復号鍵生成情報$kb = x^b$に対して、
$(kb)^a = x^{ab}$
を計算し、これをコンテンツ復号鍵を復号する情報利用装置２０２０との間での共有鍵K_{AB}とする。

【０２１１】
さらに、ライセンス情報更新装置２００８は、更新したライセンス情報の中に図６０に示したように、ライセンス情報更新装置２００８自身が生成した共有鍵生成情報ｋａ、すな

わちx^aを含める。そして、この更新されたライセンス情報は、復号部２００２、判定部２００３などを経て情報利用装置２０２０に送られる。

【０２１２】

情報利用装置２０２０では、そこで予め保持されている各情報利用装置にユニークな整数ｂと、復号ユニットＢから送られてきた復号鍵生成情報ｋａとから、

$(ka)^b=(xa)^b=x^{ab}=K_{AB}$

という計算で共有鍵K_{AB}を得ることができる。

【０２１３】

これにより、たとえ復号ユニットＢの秘密鍵が読み取られても復号ユニットＢの情報だけからではコンテンツ復号鍵を得ることはできない。

【０２１４】

何故ならば、共有鍵の生成情報としてｋａ＝x^a、ｋｂ＝x^bが存在するが、これらから$K_{AB}=x^{ab}$を構成することは計算量的に困難である。というのは、そのためにはどうしても整数ａ、ｂをもとめる必要があるが、x^aと公開されているｘとからａを求める問題は離散対数問題と呼ばれ、離散対数問題を安全性の根拠とする公開鍵暗号（例えば楕円曲線暗号）においては計算量的に困難であるからである。かくして、復号ユニットＢ内でコンテンツ復号鍵が未暗号化データとして存在する状態を解消することができ、復号ユニットＢ内部に存在する不可情報ｗ復号するための秘密鍵が読み出されてもコンテンツ復号鍵ｋｃが取り出せないシステムが実現した。

【０２１５】

さて、図６１の説明に戻り、ライセンス更新のため当該コンテンツを利用する情報利用装置２０２０は、共有鍵生成情報抽出部２０３１からの要求に応じて鍵生成情報ｋｂを出力し、共有鍵生成情報抽出部２０３１ではこれを受けて、更新情報生成部２００４に鍵生成情報ｋｂを送る（ステップＳ１０３７）。これと並行して、共有鍵生成情報抽出部２０３１は利用条件入力部２００９を起動し、ユーザに対して希望利用条件の入力を促し、更新情報生成部２００４では、入力された希望利用条件と別途得られているコンテンツＩＤや鍵生成情報ｋｂなどからライセンスの更新情報を生成して（図６２参照）、例えば、所定の通信回線（インターネットでもよい）を経由してライセンス情報更新装置２００８に送信する（ステップＳ１０３８～ステップＳ１０４０）。

【０２１６】

なお、前述の公開鍵および秘密鍵を個別に保持もしくは生成する復号ユニットＡの機能と、コンテンツ復号鍵をライセンス情報更新装置２００８と情報利用装置２０２０との間の共有鍵で暗号化するように構成された復号ユニットＢの機能とを組み合わせた復号ユニットＣも構成できることは自明であろう。

【０２１７】

この場合、復号ユニットＣには、図６０に示したようなライセンス情報が復号ユニットＣから通知された公開鍵にて暗号化されたものが、図６３に示したような復号ユニットＣに入力する。なお、図６３において、図５４の復号ユニットＡと同一部分は同一符号を付し、異なる部分は、更新情報生成部２００４が、ライセンス更新の際に、情報利用装置２０２０に対しアクセスして、情報利用装置２０２０が保持する鍵生成情報ｋｂを取得し、図６４に示すような、少なくとも該取得された鍵生成情報ｋｂ、鍵生成部２００６で生成された公開鍵、入力された希望利用条件、コンテンツＩＤを含むライセンスの更新情報を生成し、ライセンス情報更新装置２００８に送信する点である。

（３）　復号ユニットＤ

復号ユニットＤは、前述の復号ユニットＡ、Ｂとは異なり、復号鍵がライセンス情報更新装置２００８との間で１回限り利用される共有鍵である。すなわち、復号鍵は復号する際に、その都度生成し、復号ユニットＤ内に復号鍵を保持しなくても良い。これは秘密にするべき復号鍵が一時的に作られ、使われた後はすぐメモリ上から消去できることを意味し、復号ユニットの安全性向上の点から有効である。

【０２１８】

図６６は、復号ユニットＤに入力されるライセンス情報の一例を示したもので、図６６に示すように、暗号化部分と未暗号化部分で構成されている。暗号化部分は、少なくともコンテンツ利用条件、コンテンツ復号鍵ｋｃ、コンテンツＩＤからなっており、全体を復号ユニットＤとライセンス情報更新装置２００８との間の共有鍵K_{AB}で暗号化されている。未暗号化部分は、少なくとも共有鍵K_{AB}を生成するためにライセンス情報更新装置２００８が生成した共有鍵生成情報ｋａと復号ユニットＤが以下に述べる方法で生成する共有鍵生成情報ｋｂから構成される。なお、共有鍵K_{AB}の生成方法は前述の復号ユニットＢでの説明と同様である。

【０２１９】

図６５は、復号ユニットＤの構成例を示したものである。図６７に示すフローチャートを参照して、図６５の復号ユニットＤの各構成部の動作について説明する。

【０２２０】

ライセンス情報はライセンス情報入力部２００１を介して入力される（ステップＳ１０５１）。入力されたライセンス情報は、ライセンス情報入力部２００１で暗号化部分と未暗号化部分とに分けられ、暗号化部分は復号部２００２に送られ、未暗号化部分にある共有鍵生成情報ｋａ、ｋｂは、復号鍵生成部２０４１に送られる（ステップＳ１０５２１）。

【０２２１】

復号鍵生成部２０４１は、共有鍵生成情報ｋｂを共有鍵生成情報生成部２０４２に送り、共有鍵生成情報生成部２０４２に格納されているテーブル２０４３を参照して、共有鍵生成情報ｋｂに対応する共有鍵情報ｂを取得する（ステップＳ１０５３～ステップＳ５４）。これを受けて復号鍵生成部２０４１は共有鍵生成情報ｋａ、ｂとから共有鍵K_{AB}を生成する（ステップＳ１０５５）。

【０２２２】

共有鍵K_{AB}は復号部２００２に送られ、ライセンス情報の暗号化部分の復号に用いられる（ステップＳ１０５６）。

【０２２３】

復号されたライセンス情報は判定部２００３に送られ、ここで利用条件のチェックが行われる（ステップＳ１０５７）。その結果、コンテンツの利用が可能と判定された場合は、コンテンツ復号鍵ｋｃを情報利用装置２０２０に出力する（ステップＳ１０５８～ステップＳ１０５９）。コンテンツの利用が不可と判定された場合、その旨を受けた更新情報生成部２００４が共有鍵生成情報生成部２０４２に対し、共有鍵生成情報の生成を指示する。

【０２２４】

共有鍵生成情報生成部２０４２では、これを受けて共有鍵情報ｂと共有鍵生成情報ｋｂのペアを生成し、共有鍵生成情報生成部２０４２内部に具備されたメモリに格納されているテーブル２０４３に登録する（ステップＳ１０６０）。また、ここで生成された共有鍵生成情報ｋｂは、更新情報生成部へ２００４送られる。

【０２２５】

一方、更新情報生成部２００４は、希望利用条件の入力を利用条件入力部２００９へ促し、利用条件入力部２００４では然るべきヒューマンインタフェースを利用して、ユーザから希望利用条件の入力を受け、それを更新情報生成部２００４に送る。

【０２２６】

更新情報生成２００４では、以上の過程で得られた情報を基に図６９に示すような更新情報を生成し、所定の通信回線を介してライセンス情報更新装置２００８に送信し、更新されたライセンス情報の発行を受けることになる（ステップＳ１０６１～ステップＳ１０６３）。

【０２２７】

ライセンス情報更新装置２００８では、前述同様、共有鍵生成情報ｋａを生成するとともに共有鍵K_{AB}を生成して、図６６の共有鍵生成情報ｋａを該生成された共有鍵生成情報ｋａに更新し、また、共有鍵生成情報ｋｂを更新情報に含まれていた共有鍵生成情報ｋｂに

更新するとともに、更新情報に含まれていた希望利用条件に基づき更新された利用条件等を該生成された共有鍵K_{AB}で暗号化してライセンス情報を更新する。

【０２２８】

さて、復号ユニットＤでコンテンツを最初に利用再生する場合は、（共有鍵生成情報ｋｂが生成されていないので）復号鍵生成部２０４１では、共有鍵K_{AB}が生成できない）のでライセンス情報を復号することができない（ステップＳ１０５３）。

【０２２９】

この場合の処理について、図６８に示すフローチャートを参照して説明する。この場合、当該ライセンス情報の未暗号化部分には、共有鍵生成情報ｋｂが存在しない（もしくはＮＵＬＬコードなどの無効な情報が入っている）ことで最初の利用再生であることを復号鍵生成部２０４１が検知し、共有鍵生成情報生成部２０４２に対し共有鍵生成情報を作成する旨の指示を行なう。これを受けて、共有鍵生成情報生成部２０４２では、共有鍵情報ｂと共有鍵生成情報ｋｂのペアを生成し、共有鍵生成情報ｋｂとライセンスを更新する旨の指示を更新情報生成部２００４へ送る（ステップＳ１０７１）。

【０２３０】

この場合、ライセンス情報の暗号化部分は（全ての復号ユニットＤに共通に使われている）秘密鍵ｋｓで暗号化されている。復号部２００２では、復号鍵生成部２０４１からこの秘密鍵ｋｓの出力を受け、暗号化部分を復号する（ステップＳ１０７２）。復号されたライセンス情報の暗号化部分からコンテンツＩＤを抽出する（ステップＳ１０７３）。

【０２３１】

更新情報生成部２００４では、これを受けて希望利用条件の入力を利用条件入力部２００９へ促して、希望利用条件入力部２００９を介してユーザからの希望利用条件の入力を受ける（ステップＳ１０７４）。更に以上の過程で得られたコンテンツＩＤ、希望利用条件と共有鍵生成情報ｋｂを図６９に示すような更新情報の予め定められたフォーマットにまとめ、これをライセンス情報更新装置２００８に送信する（ステップＳ１０７５）。これにより更新されたライセンス情報が発行されることとなる。

【０２３２】

このような最初の利用再生である場合は、ライセンス情報の暗号化部分に有効なコンテンツ復号鍵を入れないようにすると、さらに安全性が向上する。すなわち、もともとのライセンス情報にコンテンツ復号鍵が含まれていなければ、例え共通の秘密鍵ｋｓが露見してもコンテンツ復号鍵は抽出できないので安全であるからである。この場合の暗号化は、コンテンツＩＤの変更を阻止するためのものであるといえる。

【０２３３】

以上のようにすることによって、復号の度に復号鍵K_{AB}を生成し、ライセンス情報が更新される度に異なる復号鍵K_{AB}で復号しなければならなくなるので（ライセンス情報に含まれる復号鍵生成情報ｋｂに応じてテーブル２０４３から検索された復号鍵情報ｂにて異なる復号鍵が生成されるので）、復号鍵K_{AB}が露見した場合の影響が少なくなる。そればかりか公開鍵暗号に比べ格段に高速である共有鍵暗号が使えるのでライセンス情報のデータサイズを大きくしても実時間で復号し、ライセンス情報に含まれる利用条件に基づくコンテンツの利用可否の反映が行えるという利点がある。

【０２３４】

次に、復号ユニットＤのバリエーションについて述べる。

【０２３５】

まず、復号ユニットＤが生成する共有鍵生成情報ｋｂは固定であってもよい。この場合、安全性は少々落ちるが、ライセンス情報更新装置２００８の作成する共有鍵生成情報ｋａが毎回変われば共有鍵K_{AB}は毎回変わるので、復号ユニットＤの有効性は保たれる。また、図６５に示す共有鍵生成情報生成部２０４２は不要となり、予め定められた共有鍵生成情報ｋｂ、共有鍵情報ｂを復号鍵生成部２０４１に持たせておけばよい。

【０２３６】

また、復号ユニットＤで最初にコンテンツ情報を利用再生する場合、図６８に示したよう

に、必ず共有鍵生成情報ｋｂの取得に伴うライセンスの更新をしなければならないという問題があった。この問題を解決するために初回のライセンス情報に限っては、予め定められた共有鍵K_{com}か、公開鍵K_pで暗号化するという方法が考えられる。この場合、共有鍵K_{com}もしくは公開鍵K_pに対応する秘密鍵K_pを復号ユニットＤ内に保持している必要があり、初回だけそれを用いる。前述の図６８に示した最初の利用再生時の処理動作と異なる点は、図６８の場合、コンテンツ復号鍵を含めなくても良いが、今回の場合には必ず含めなくてはいけないという点である。

【０２３７】

すなわち、図６７のステップＳ１０５３において、復号鍵生成部２０４１で共有鍵成情報ｋａ、ｋｂが存在しないことで、初回の利用再生であると判断し、復号鍵生成部２０４１もしくは復号部２００２にある共有鍵K_{com}もしくは秘密鍵K_pを用いて復号部２００２がライセンス情報を復号する。その後は、図６７のステップＳ１０５４以降と同様である。

【０２３８】

さらに、復号ユニットＤが生成している共有鍵生成情報ｋｂを情報利用装置２０２０に作らせる方法も考えられる。この場合の復号ユニットＤ’の構成を図７０に示す。図７０に示すように、図６５の共有鍵生成情報生成部２０４２が情報利用装置２０２０に置き換わる。もっとも情報利用装置２０２０は、復号ユニットＤ’の外部にあるので共有鍵情報ｂは秘密にしなければならないが、これは復号鍵生成部２０４１と情報利用装置２０２０との間の一時鍵による暗号化によって解決できる。この場合、共通鍵情報ｂですら復号ユニットＤ’内に保持しないことになり、復号ユニットＤより安全になる。しかし、このような場合は情報利用装置２０２０の方も攻撃の対象になるが、それは情報利用装置個々によって実装の仕方が違うので個別の対応が必要であり、情報利用装置２０２０によって安全性のレベルを変えることもできる。尚、復号ユニットＤ’の処理動作は、図６７、図６８に示したフローチャートと同様である。

（４）　復号ユニットＡに対応するライセンス情報更新装置

図７１は、前述の復号ユニットＡに対応するライセンス情報更新装置２００８の構成例を示したものである。以下、図７２に示すフローチャートを参照して、図７１のライセンス情報更新装置２００８の各構成部の処理動作について説明する。

【０２３９】

復号ユニットＡから送信されるライセンスの更新情報は、更新情報入力部２０５１を介しライセンス情報更新装置２００８に入力する（ステップＳ１０８１）。

【０２４０】

ここで用いられる更新情報は、図５６に示した更新情報で、希望利用条件、コンテンツＩＤ、復号ユニットＡで生成された公開鍵などが含まれた、ライセンスの更新に必要な情報である。この中で、コンテンツＩＤは利用許可を与えるコンテンツを特定するためのものであり、これによってライセンス情報更新装置２００８の持つデータベースを使って希望利用条件にあった課金情報が取得でき、更に当該コンテンツ復号鍵もデータベースを使って取得できるのである。このためライセンス情報更新装置２００８には、ライセンス情報を更新するためにコンテンツ復号鍵を入力する必要はなく、従って図５６の更新情報は暗号化して送る必要もない。この点も図７２に示したライセンス情報更新装置２００８の特徴である。

【０２４１】

さて、更新情報入力部２０５１から入力した図５６に示したような更新情報は、料支払要求部２０５２に送られ、ここから、更新情報に含まれている希望利用条件が料金問い合わせ部２０５７に送られる。

【０２４２】

料金問い合わせ部２０５７では、料金データベース（ＤＢ）２０５８にアクセスして、希望利用条件に対応した料金を取得する（ステップＳ１０８２～ステップＳ１０８３）。例えば、希望利用条件として２ヶ月という有効期間が指定されていたら、その期間に見合ったコンテンツＩＤのコンテンツの利用料金値が検索されて、料金問い合わせ部２０５７、

さらに、料金支払要求部２０５２に渡される。

【０２４３】

料金支払要求部２０５２は、取得した料金値と更新情報に含まれる当該顧客に関するデータとを基に、所定の通信回線を介して所定の電子決済システム２０６０にアクセスして当該顧客からの料金の支払要求を行う。電子決済システム２０６０は、所定の電子支払処理を実行する（ステップＳ１０８４）。

【０２４４】

ライセンス情報更新装置２００８の支払い確認部２０５３は、所定の通信回線を介して、電子決済システム２０６０と交信して、料金の支払いが確認されると、次に、コンテンツ復号鍵取得部２０５４での処理に以降する（ステップＳ１０８５）。

【０２４５】

コンテンツ復号鍵取得部２０５４では、コンテンツＩＤをキーにしてコンテンツ復号鍵データベース（ＤＢ）２０５９を検索し、コンテンツ復号鍵を取得する（ステップＳ１０８６）。なお、ライセンス情報更新装置２００８は、特定の信頼できる業者が管理運営していると考えているので、コンテンツ復号鍵ＤＢ２０５９内も得られたコンテンツ復号鍵も特に暗号化する必要はない。

【０２４６】

次に、ライセンス情報暗号化部２０５５では、上記得られた情報を基にライセンス情報を構築し（ステップＳ１０８７）、そのライセンス情報を、先に受け取った図５６に示したような更新情報に含まれている公開鍵で暗号化し（ステップＳ１０８８）、ライセンス情報出力部２０５６を介して、ライセンス情報の更新要求元のクライアント、すなわち、復号ユニットＡに所定の通信回線を介して送信する（ステップＳ１０８９）。

（５）　復号ユニットＢに対応するライセンス情報更新装置

図７３は、前述の復号ユニットＢに対応するライセンス情報更新装置２００８の構成例を示したものである。以下、図７４に示すフローチャートを参照して、図７３のライセンス情報更新装置２００８の各構成部の処理動作について説明する。

【０２４７】

なお、図７３において、図７１と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図７３において、コンテンツ復号鍵取得部２０５４とライセンス情報暗号化部２０５５との間に共有鍵生成部２０６１とコンテンツ復号鍵暗号化部２０６２とが追加されている。また、図７４のフローチャートにおいて、図７２のフローチャートと同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、ステップＳ１０８６とステップＳ１０８７の間に、共有鍵生成部２０６１にて整数ａと共有鍵生成情報ｋａとを生成して、これらと更新情報に含まれる各情報利用装置２０２０にユニークな共有鍵生成情報ｋｂとから共有鍵K_{AB}を生成し（ステップＳ１０９１～ステップＳ１０９２）、さらに、暗号化部２０６２で、この新たに生成された共有鍵K_{AB}を用いてステップＳ１０８６で新たに取得されたコンテンツ復号鍵を暗号化する処理（ステップＳ１０９３）が追加される。

【０２４８】

図７３の構成では、コンテンツ復号鍵を暗号化してライセンス情報に入れるために共有鍵生成部２０６１において、情報利用装置２０２０とライセンス情報更新装置２００８との間で該暗号化されたコンテンツ復号鍵を復号するための共有鍵を生成する必要がある。共有鍵の生成法は復号ユニットＢの説明でも述べたように共有鍵生成情報を用いて行う。従って、図７３のライセンス情報更新装置２００８に入力される更新情報は、図６２のように、少なくとも希望利用条件とコンテンツＩＤと情報利用装置２０２０が乱数等を使って生成した共有鍵生成情報ｋｂが含まれている。

【０２４９】

ステップＳ１０８８では、ライセンス情報暗号部２０５５にて新たに生成されたライセンス情報が予め定められた公開鍵で暗号化される。

【０２５０】

なお、前述の公開鍵および秘密鍵を個別に保持もしくは生成する復号ユニットＡの機能と、コンテンツ復号鍵をライセンス情報更新装置２００８と情報利用装置２０２０との間の共有鍵で暗号化するように構成された復号ユニットＢの機能とを組み合わせた復号ユニットＣに対応するライセンス情報更新装置の場合、入力される更新情報には、さらに復号ユニットＣで生成された公開鍵を含み、図７４のステップＳ１０８８では、当該公開鍵を用いて生成されたライセンス情報を暗号化すればよい。

【０２５１】

また、復号ユニットＤ、Ｄ’に対応するライセンス情報更新装置も図７３とほぼ同様で、異なるのは、図７３の暗号化部２０６２では、利用条件とコンテンツ復号鍵ｋｃ、コンテンツＩＤとを共有鍵K_{AB}を用いて暗号化し、図６６に示したようなライセンス情報を生成し、その生成されたライセンス情報は、そのままライセンス情報出力部２０５０を介して出力されることである。

（第３の実施形態）

第３の実施形態に係る情報流通システムの構成例を図７５に示す。

【０２５２】

図７５において、利用者はＤＶＤ等のリムーバブル情報蓄積メディア（以下、簡単にメディアと呼ぶ）に記録された課金対象であるコンテンツ情報を入手する。当該コンテンツ情報に対するライセンス情報もまた当該メディアに記録されている。利用者の情報再生装置には、復号ユニットが内蔵され、メディアから読み出されたライセンス情報に基づき当該コンテンツ利用の可否を判定するようになっている。

【０２５３】

コンテンツ利用が不可の場合に、利用者が当該コンテンツを利用するためには、ライセンス情報の更新を受けなければならない。すなわち、コンテンツの利用が可能となるように、ライセンス情報に含まれる利用条件を更新、すなわち、ライセンスの更新を行う必要がある。この利用条件、ひいてはライセンス情報の更新を行うのは、例えば、そのためのライセンス更新端末を有する店舗で行われる。ライセンス更新端末はライセンス販売代行業者が運営するライセンスサーバに接続されている。利用者は所望の利用条件（例えば、コンテンツの指定とその利用期間等）を指定して、それに応じたライセンス料金（利用条件に見合うコンテンツの利用料金）を店舗に支払う。すると、ライセンス更新端末はライセンスサーバと交信して、ライセンスサーバから送られてくる情報に基づきメディアに記録されているライセンス情報が更新されることにより、ライセンスが更新される。例えば、利用者が期限付きライセンスを購入した場合、利用期限満了迄ライセンス更新を行うこと無くコンテンツを利用する事ができる。

【０２５４】

図７６は、情報流通システムの他の構成例を示したものである。図７５と異なる点は、少なくとも復号ユニットの機能がＩＣカード等のカード型の記録媒体に内蔵されている。以下、復号ユニットを内蔵したＩＣカード等のカード型記録媒体を復号判定カードと呼ぶ。この場合、利用者はライセンスを更新する際、復号判定カードをライセンス更新端末を有する店舗に携帯する。ライセンス更新端末は復号判定カードから公開マスターキーを読み取り、ライセンスサーバーに転送する。利用者は所望の利用条件（例えば、コンテンツの指定とその利用期間等）を指定して、それに応じたライセンス料金（利用条件に見合うコンテンツの利用料金）を店舗に支払う。すると、ライセンス更新端末はライセンスサーバーと交信して、ライセンスサーバーから送られてくる情報に基づきメディアに記録されているライセンス情報が更新され、ライセンスが更新される。

【０２５５】

なお、公開マスターキーについては後述する。

【０２５６】

また、図７５において、復号ユニットは、情報再生装置に内蔵されている場合にのみ限らず、図７６の復号判定カードのような形態であって、情報再生装置に着脱可能に装着されていてもよく、以下、図７５、図７６の情報流通システムについて、復号判定カードを用

いる場合を例にとり説明する。
（１）
以下、図７５の情報流通システムについて説明する。
（１－１）情報再生装置
図７７は、復号判定カードを装着した情報再生装置の要部の構成例を示したもので、バス３００７に復号判定カード３００１、メディア読取装置３００３、情報再生装置３００４、時計３００５、央処理装置３００６が接続されて構成されている。
【０２５７】
時計３００５は、利用条件としてのコンテンツの利用期限を有効／無効を判定するためのもので、前述の第１の実施形態で説明したように、暗号化コマンドによる時刻設定を行うことを特徴としている。ライセンス更新の際には、この時計の時刻をサーバーの時刻に合わせる、時刻設定動作を行う。この動作については、前述した通りである。これによって、時計３００５の時刻をほぼ正確に維持する事が可能となる。
【０２５８】
メディア読取装置３００３は、ＤＶＤ等のメディア３００２に記録された情報を読み取り、この読み取られた情報に基づき復号判定装置３００１でメディア３００２に記録されたコンテンツ情報の利用の可否を判定し、利用可と判定された場合は情報再生部３００４は、メディア読取装置３００３でメディア３００２から読み取られたコンテンツ情報を再生できるようになっている。中央処理装置３００６は上記各部の動作を制御するためのものである。
【０２５９】
図７７の復号判定カード３００１と時計３００５とは、それぞれ鍵生成情報Ｋｔを保持している。また、復号判定カード３００１と情報再生装置３００４とは、それぞれ鍵生成情報Ｋ’ｔを保持している。
【０２６０】
乱数Ａ、Ｂおよび鍵生成情報Ｋｔに基づき、時計３００５と復号判定カード３００１との間で現在時刻情報を転送する際に該情報の暗号化／復号化のために１回限り有効な転送キーＫＴが生成される。また、乱数Ｃ、Ｄおよび鍵生成情報Ｋ’ｔに基づき、復号判定カード３００１と情報再生部３００４との間で暗号化されたコンテンツ情報を復号するコンテンツキーＫｃを転送する際に、該コンテンツキーＫｃの暗号化／復号化のために１回限り有効な転送キーＫＴが生成される。これによって、バス３００７を流れる情報データが保護される。
【０２６１】
メディア３００２には、次の様な情報が格納されている。
・マスターキーＫＭによって暗号化されたライセンス情報（［ライセンス情報］ＫＭ）
・ライセンス情報を復号するためのマスターキーＫＭを指定する識別子（例えば、番号）であるマスターキーＩＤ
・コンテンツキーＫｃによって暗号化されたコンテンツ情報（［コンテンツ］Ｋｃ）
なお、以下の説明では、ライセンス情報を暗号化／復号化の際に用いる暗号キーと復号キーとを合わせてマスターキーＫＭと呼び、ライセンス情報の暗号キーと復号キーとが必ずしも同じキーであるとは限らない。
【０２６２】
ライセンス情報は、次の様な情報から構成されている。
・コンテンツキーＫｃ
・コンテンツＩＤ
・利用期限、利用開始時刻、及びライセンス情報記録時刻等のコンテンツの利用条件
図７８に示すフローチャートは、図７５の情報流通システムで用いられる図７７の情報再生装置の処理動作を示したものである。
【０２６３】
まず、メディア読取装置３００３は、そこにセットされたメディア３００２からマスター

キーＩＤ、［ライセンス情報］ＫＭを読み取り、復号判定カード３００１に、それらを転送する（ステップＳ３００１～ステップＳ３００２）。

【０２６４】

時計３００５は、所定のアルゴリズムにて乱数Ａを発生して、それを復号判定カード３００１に転送する（ステップＳ３００３）。一方、復号判定カード３００１も所定のアルゴリズムにて乱数Ｂを発生し、時計３００５に転送する（ステップＳ３００４）。これにより、復号判定カード３００１と時計３００５は互いに乱数Ａ、Ｂを確認し合うこととなる。

【０２６５】

復号判定カード３００１および時計３００５は、乱数Ａ、Ｂ、および自らが保持している鍵生成情報Ｋｔから転送キーＫＴを生成する（ステップＳ３００５、ステップＳ３００６）。時計３００５は生成された転送キーＫＴで、現在の時刻情報を暗号化し（［現在時刻］ＫＴ）、それを復号判定カード３００１へ転送する（ステップＳ３００７）。

【０２６６】

復号判定カード３００１では、［ライセンス情報］ＫＭをマスターキーＩＤにて指定されたマスターキーＫＭを用いてライセンス情報を復号し、また、時計３００５から転送されてきた［現在時刻］ＫＴを生成された転送キーＫＴで復号し、復号されたライセンス情報と復号された時刻情報とに基づき、コンテンツＩＤにて指定されるコンテンツ情報の利用の可否、すなわち、復号の可否を判定する（ステップＳ３００８）。復号が不可と判定されたときは、処理を終了する。

【０２６７】

復号が可能と判定されたときは（ステップＳ３００９）、復号判定カード３００１は所定のアルゴリズムにて乱数Ｃを発生し、それを情報再生部３００４に転送する（ステップＳ３０１０）。情報再生部３００４も所定のアルゴリズムにて乱数Ｄを発生する（ステップＳ３０１１）。これにより、復号判定カード３００１と情報再生部３００４は互いに乱数Ｃ、Ｄを確認し合うこととなる。

【０２６８】

復号判定カード３００１および情報再生部３００４は、乱数Ｃ、Ｄ、および自らが保持している鍵生成情報Ｋ’ｔから転送キーＫ’Ｔを生成する（ステップＳ３０１２、ステップＳ３０１３）。復号判定カード３００１は、生成された転送キーＫ’Ｔでライセンス情報に含まれていたコンテンツキーＫｃを暗号化して（［Ｋｃ］Ｋ’Ｔ）、それを情報再生部３００４へ転送する（ステップＳ３０１４）。

【０２６９】

メディア読取装置３００３は、メディア３００２から［コンテンツ］Ｋｃを読み取り、それを情報再生部３００４へ転送する（ステップＳ３０１５）。

【０２７０】

情報再生部３００４は、［Ｋｃ］Ｋ’Ｔを生成された転送キーＫ’Ｔで復号し、その結果得られたコンテンツキーＫｃでコンテンツ情報を復号する（ステップＳ３０１６）。

（１－２）復号判定カード

図７９は、復号判定カード３００１の構成例を示したものである。

【０２７１】

時刻転送部３０１２は、図７７の情報再生装置に具備される時計３００５でカウントされている時刻情報を受け取り、復号判定部３０１３に転送するためのものである。

【０２７２】

コンテンツキー転送部３０１４は、図７７の情報再生部３００４へのコンテンツキーＫｃの転送保護の為の動作を行う。

【０２７３】

データ転送部３０１１は、時計３００５から転送される時刻情報、情報再生部３００４へ転送するコンテンツキー以外の情報を、メディア読取装置３００３、情報再生部３００４、復号判定カード３００１との間でやりとりする際に用いられる。

【０２７４】
時刻転送部３０１２とデータ転送部３０１１とを別個に設けるのは、時刻転送に伴って、一時キーによるデータ保護とクロックによるタイムアウトなど特別な処理が行われる為である。
【０２７５】
図８０に示すフローチャートは、図７９の復号判定カード３００１における、コンテンツ情報の利用可否の判定結果を出力するまでの処理動作をより詳細に示したものである。
【０２７６】
図７８のステップＳ３００２でメディア読取装置３００３から転送されたマスターキーＩＤ、［ライセンス情報］ＫＭは、データ転送部３０１１を介して復号判定部３０１３に入力する（ステップＳ３０２１）。また、図７８のステップＳ３００３で時計３００５から転送された乱数Ａは、時刻転送部３０１２に入力する（ステップＳ３０２２）。これを受けて、時刻転送部３０２２は、乱数Ｂを発生し、この乱数Ｂと先に受け取った乱数Ａとから転送キーＫＴを生成する（ステップＳ３０２３～ステップＳ３０２４）。乱数Ｂを時計３００５に転送する（ステップＳ３０２５）。これと同時に、時刻転送部３０２２は、クロックカウンタのカウントを開始する（ステップＳ３０２６）。
【０２７７】
図７８のステップＳ３００７で時計３００５から転送された［現在時刻］ＫＴは時刻転送部３０２２に入力したとき（ステップＳ３０２７）、時刻転送部３０２２のカウンタ値が予め定められた値Ｃｔ以内でないときは処理を終了する（ステップＳ３０２８）
カウンタ値Ｃｔは、タイムアウト時間で、予め定められた正整数である。本実施形態の場合、復号判定カードは時刻情報を復号判定カード３００１の外部から取得する。従って、取得した時刻情報の正当性が問題になる。時計３００５と復号判定カード３００１の時刻転送部３０１２との間で乱数Ａ、Ｂを交換し、一度限り有効な鍵ＫＴで時刻情報を暗号化して転送するのは、その為である。しかし、それだけでは、時刻情報の転送を意図的に遅延させるという不正に対して対処できない。
【０２７８】
そこで、時刻転送部３０１２は、時刻情報の到着時間、すなわち、時刻転送部３０１２が乱数Ｂを出力してから（暗号化された）時刻情報が時刻到着部３０１２に到着するまでの時間が、一定の時間Ｃｔ以内でなければ処理を停止することによって、この種の不正を防ぐことができる。
【０２７９】
［現在時刻］ＫＴの入力が所定時間以内であれば、それを先に生成された転送キーＫＴで復号して時刻情報を得る（ステップＳ３０２９）。時刻情報は復号判定部３０１３に転送され、復号判定部３０１３では、復号されたライセンス情報と復号された時刻情報とに基づき、コンテンツＩＤにて指定されるコンテンツ情報の利用の可否、すなわち、復号の可否を判定する（ステップＳ３０３１）。復号が不可と判定されたときは、処理を終了する。
【０２８０】
復号が可能と判定されたときは（ステップＳ３０３２）、復号判定部３０１３はライセンス情報に含まれていたコンテンツキーｋｃをコンテンツキー転送部３０１４に出力する（ステップＳ３０３３）。
【０２８１】
コンテンツキー転送部３０１４は乱数Ｃを発生すると、それを情報再生部３００４に転送する（ステップＳ３０３４）。そして、図７８のステップＳ３０１１で情報再生部３００４から転送された乱数Ｄがコンテンツキー転送部３０１４に入力すると、この乱数Ｄと乱数Ｃとから転送キーＫ’Ｔを生成する（ステップＳ３０３５～ステップＳ３０３６）。コンテンツキー転送部３０１４は、生成された転送キーＫ’Ｔを用いてコンテンツキーＫｃを暗号化して（［Ｋｃ］Ｋ’Ｔ）、それを情報再生装置３００４へ転送する（ステップＳ３０３８）。

（１－３）復号判定カードの時刻転送部
次に、図７９の時刻転送部３０１２についてより詳細に説明する。図８１は、時刻転送部３０１２の構成例を示したもので、認証部３０２１とクロックカウンタ３０２３と時刻出力部３０２２とから構成されている。
【０２８２】
図８１において、クロックカウンタ３０２３は、ロジック駆動用のクロックを数える計数カウンタである。
【０２８３】
図８２は、図８１の認証部３０２１の構成例を示したものである。
【０２８４】
図８２において、秘密鍵格納部３０２１ｅは、鍵生成情報Ｋｔを保持している。
【０２８５】
転送鍵生成部３０２１ｆは適当なアルゴリズムによって、乱数Ａ、Ｂ及び鍵生成情報Ｋｔから、秘密鍵としての転送キーＫＴを生成する。このアルゴリズムは、対応する時計３００５の認証部における秘密鍵生成アルゴリズムと同一であり、従って、復号判定カード３００１と時計３００５は転送キーＫＴを共有することができる。
【０２８６】
予め定められたカウンタ値Ｃｔは入出力部３０２１ａが保持しており、クロックカウンタ３０２３の値を参照してタイムアウトを判定する。Ｃｔの値には、時計３００５が乱数Ｂを受け取ってから暗号化した時刻情報を返す迄に必要なクロック数に、転送の為の若干の余裕を持たせた値を設定する。
【０２８７】
図８３は、図８２に示した認証部の処理動作を説明するためのフローチャートである。
【０２８８】
図８０のステップＳ３０２２で時刻転送部３０１２に入力された乱数Ａは、まず、認証部３０２１の入出力部３０２１ａに入力し（ステップＳ３０４１）、乱数Ａは乱数格納部３０２１ｂに格納される（ステップＳ３０４２）。次に、乱数発生部３０２１ｃは、所定のアルゴリズムにて乱数Ｂを発生し（ステップＳ３０４２）、乱数格納部３０２１ｄに格納するとともに、乱数Ｂを入出力部３０２１ａに転送する（ステップＳ３０４５）。
【０２８９】
転送鍵生成部３０２１ｆは、乱数格納部３０２１ｂ、３０２１ｄのそれぞれに格納された乱数Ａ、Ｂと、秘密鍵格納部３０２１ｅに格納されている鍵生成情報ｋｔとを読み出して転送キーＫＴを生成し（ステップＳ３０４６）、転送鍵格納部３０２１ｇに格納する（ステップＳ３０４７）。
【０２９０】
入出力部３０２１ａはクロックカウンタ３０２３をリセットするとともに乱数Ｂを時計３００５に転送する（ステップＳ３０４８～ステップＳ４９）。
【０２９１】
図８０のステップＳ３０２７で時刻転送部３０１２に入力された［現在時刻］ＫＴは、まず、入出力部３０２１ａに入力する（ステップＳ３０５０）。入出力部３０２１ａはクロックカウンタ３０２３のカウンタ値を読み出し、Ｃｔと比較し、カウンタ値がＣｔ以下のときはステップＳ３０５３に進み、Ｃｔを越えているとき（タイムアウト時）は処理を終了する（ステップＳ３０５１～ステップＳ３０５２）。
【０２９２】
ステップＳ３０５３では、［現在時刻］ＫＴを復号部３０２１ｈに転送し、
復号部３０２１ｈは転送鍵格納部３０２１ｇから転送キーＫＴを読み出して、転送キーＫＴで［現在時刻］ＫＴを復号し、現在時刻情報を得る（ステップＳ３０５３～ステップＳ３０５４）。
【０２９３】
データ形式確認部３０２１ｉは、現在時刻情報のデータ形式を確認する（ステップＳ３０

５５）。現在時刻情報のデータ形式は、例えば、次のようなものである。
【０２９４】
「現在時刻」／現在時刻／「００００００００」
「現在時刻」という文字列に続き、文字列で表現された現在時刻、最後の１バイトのデータ「０」は区切り記号である。現在時刻は、西暦１９９８年１月１日午前零時からの経過時間を分単位で表したものとする。
【０２９５】
データ形式確認部３０２１ｉは、現在時刻情報のデータ形式が上記のような予め定められた形式を満足している場合のみ、該現在時刻情報を時刻出力部３０２２に出力する（ステップＳ３０５６）。
【０２９６】
時刻出力部３０２２は、時刻情報を復号判定部３０１３に出力する（図８０のステップＳ３０３０）。
【０２９７】
なお、現在時刻情報の転送の際には、暗号化用のキーと復号用のキーが同一（ＫＴ）である様な暗号化方式を採用したが、この場合に限らず、異なるキーを用いるようにしても、上記同様の構成および動作で転送保護を実現することができる。
（１－４）復号判定部のコンテンツキー転送部
次に、図７９のコンテンツキー転送部３０１４についてより詳細に説明する。図８４は、コンテンツキー転送部３０１４の構成例を示したもので、認証部３０３１とコンテンツキー入力部３０３２とから構成されている。
【０２９８】
図８５は、認証部３０３１の構成例を示したもので、図８６に示すフローチャートを参照して、認証部３０３１の処理動作について説明する。
【０２９９】
乱数発生部３０３１ｃは、例えば所定のアルゴリズムにて乱数Ｃを発生して、乱数Ｃを乱数格納部３０３１ｄに格納すると同時に（ステップＳ３０６１）、入出力部３０３１ａを介して情報再生部３００４に転送される（ステップＳ３０６２）。
【０３００】
情報再生部３００４から転送されてきた乱数Ｄが入出力部３０３１ａを介して入力すると乱数格納部３０３１ｂに格納される（ステップＳ３０６４）。
【０３０１】
転送鍵生成部３０３１ｆは、乱数格納部３０３１ｂ、３０３１ｄのそれぞれに格納されている乱数Ｃ、Ｄと、秘密鍵格納部３０３１ｅに格納されている鍵生成情報Ｋ’ｔとを読み出して転送キーＫ’Ｔを生成し、それを転送鍵格納部３０３１ｇに格納する（ステップＳ３０６５～ステップＳ３０６６）。
【０３０２】
図８０のステップＳ３０３２にて、復号判定部３０１３における復号判定の結果、復号可と判定された場合、復号判定部３０１３は、コンテンツキーＫｃをコンテンツキー転送部３０１４に転送する（図８０のステップＳ３０３３）。このコンテンツキーＫｃは、図８５の暗号化部３０３１ｈに入力し、さらに、暗号化部３０３１ｈは、転送鍵格納部３０３１ｇから転送キーＫ’Ｔを読み出して、これを用いてコンテンツキーＫｃを暗号化し（［Ｋｃ］Ｋ’Ｔ）、入出力部３０３１ａを介して情報再生部３００４に転送する（ステップＳ３０６９）。
（１－５）時計
図８７は、図７７の時計３００５の構成例を示したもので、認証部３０４１、時計カウンタ３０４２とから構成される。
【０３０３】
時計カウンタ３０４２は時刻をカウントするためのものである。
【０３０４】

図８８は、時計３００５の認証部３０４１の構成例を示したものである。ここで、図８９に示すフローチャートを参照して認証部３０４１の処理動作について説明する。

【０３０５】

乱数発生部３０４１ｃは、所定のアルゴリズムにて乱数Ａを発生し、乱数Ａを乱数格納部３０４１ｄに格納するとともに（ステップＳ３０７１）、入出力部３０４１ａを介して復号判定カード３００１に転送する（ステップＳ３０７２）。

入出力部３０４１ａに復号判定カード３００１から転送されてきた乱数Ｂが入力すると、乱数Ｂは乱数格納部３０４１ｄに格納される（ステップＳ３０７３）。

【０３０６】

転送鍵生成部３０４１ｆは、乱数格納部３０４１ｂ、３０４１ｄから乱数Ｂ、乱数Ａをそれぞれ読み出し、また。秘密鍵格納部３０４１ｅから鍵生成情報Ｋ’ｔを読み出して、転送キーＫ’Ｔを生成し、それを転送鍵格納部３０４１ｇに格納する（ステップＳ３０７４～ステップＳ７５）。

【０３０７】

時計カウンタ３０４２から出力される現在時刻情報は暗号化部３０４１ｈに入力する（ステップＳ３０７６）。

【０３０８】

暗号化部３０４１ｈは転送鍵格納部３０４１ｇから転送キーＫ’Ｔを読み出し、この転送キーＫ’Ｔで現在時刻情報を暗号化し（［現在時刻］Ｋ’Ｔ）、入出力部３０４１ａを介して復号判定カード３００１に転送する（ステップＳ３０７７～ステップＳ３０７８）。

（１－６）復号判定カードの復号判定部

図９０に図７９の復号判定カード３００１の復号判定部３０１３の構成例を示す。

【０３０９】

図９１に示すフローチャートを参照して図９０の復号判定部３０１３の処理動作について説明する。

【０３１０】

メディア読取装置３００３から復号判定カード３００１に転送されたマスターキーＩＤ、［ライセンス情報］ＫＭは、それぞれマスターキー選択部３０６１、復号部３０６３に入力される（ステップＳ３１０１、ステップＳ３１０３）。

【０３１１】

マスターキー選択部３０６１はマスターキーＩＤに対応する復号キーをマスターキー格納部３０６２を検索して取得し、それを復号部３０６３に転送する（ステップＳ３１０２）。

【０３１２】

マスターキー選択部３０６１に入力するマスターキーＩＤは［ライセンス情報］ＫＭを暗号化しているキーに対応する復号キーを指定するためのものである。正しいマスターキーＩＤがなければ、ライセンス情報を復号する復号キーを選択することができない。

【０３１３】

復号部３０６３は［ライセンス情報］ＫＭをマスターキーＩＤにて指定された復号キーで復号し、その結果得られたライセンス情報を判定部３０６４に転送する（ステップＳ３１０５）。

【０３１４】

判定部３０６４には、時計３００５から復号判定カード３００１の時刻転送部３０１２へ転送されて、ここで復号されて得られた現在時刻情報が時刻入力部３０６５を介して入力する（ステップＳ３１０６～ステップＳ３１０７）。

【０３１５】

判定部３０６４では、ライセンス情報と現在時刻情報とに基づきコンテンツ情報の利用可否、すなわち復号可否を判定し、判定結果出力部３０６６を介して判定結果をデータ転送部３０１１に出力する（ステップＳ３１０８～ステップＳ３１１０）。また、復号可と判定されたときは、ライセンス情報に含まれているコンテンツキーＫｃをコンテンツキー出

力部３０６７を介してコンテンツキー転送部３０１４に出力する（ステップＳ３１１１）。

【０３１６】

ここで、判定部３０６４の判定処理について説明する。時計３００５から送られる現在時刻がライセンス情報のメディア３００２への記録時刻以前であれば、それは、現在時刻が正しい時刻から遅れている事を示す。ライセンス情報記録時刻はライセンスサーバーが記録しており、従って、ほぼ正確な時刻であると考えて良いからである。従って、この場合、判定部３０６４が具備する判定フラグをクリアして、以後全ての判定を「利用不可」とする。判定フラグを再びセットして判定を有効にするには、情報再生装置の時計３００５からのコマンドを要する。このコマンドは、復号判定カード３００１の時刻転送部３０１２を経由して復号判定部３０１３に送られる。従って、正統な（認証可能な）時計３００５からのコマンドのみが、判定フラグを再設定できる。そして、時計３００５が判定フラグを再設定するのは、時計３００５の時刻が設定されたときのみである。

（１－７）マスターキー

ライセンス情報を暗号化、復号化する際に用いるマスターキーについて説明する。なお、ここでは、ライセンス情報を暗号化／復号化の際に用いる暗号キーと復号キーとを合わせてマスターキーと呼び、ライセンス情報の暗号キーと復号キーとが必ずしも同じキーであるとは限らない。

【０３１７】

図９０のマスターキー格納部３０６２におけるマスターキーは、マスターキーＩＤとともに、例えば、次のように記憶されている。

Ｋｍ（０）、…、Ｋｍ（９９９）、（ＫＰ（１０００）、Ｋｓ（１０００））、…、（ＫＰ（１４９９）、Ｋｓ（１４９９））、（ＫＰ（１５００）、Ｋｓ（１５００））、…、（ＫＰ（１５９９）、Ｋｓ（１５９９））

Ｋｍ（０）からＫｍ（９９９）迄の１０００個のキーは予め定められた復号用の秘密鍵である。ＫＰ（１０００）からＫＰ（１５９９）は、ライセンス情報暗号化用の公開鍵であり、Ｋｓ（１０００）からＫｓ（１５９９）の６００個のキーはＫＰ（１０００）からＫＰ（１５９９）のそれぞれのライセンス情報復号用の秘密鍵である。ＫＰ（ｎ）（１０００＜＝ｎ＜１６００）を公開マスターキーと呼ぶ。

【０３１８】

１０００以上１６００未満の任意のｎについて、ＫＰ（ｎ）とＫｓ（ｎ）とは対になるキーである。即ち、ＫＰ（ｎ）で暗号化されたライセンス情報はＫｓ（ｎ）によって復号できる。１０００以上１６００未満の各ｎについて、（ＫＰ（ｎ）、Ｋｓ（ｎ））の対は、図９０のマスターキー生成部３０６９によって、乱数発生部３０６８で発生される乱数に基づき随時生成される。従って、復号判定カード毎に異なっているばかりで無く、同じ復号判定カードでも時期によって異なっている。

【０３１９】

公開マスターキーは、後述するように、図７６の情報流通システムで用いられる。

【０３２０】

（ＫＰ（ｎ）、Ｋｓ（ｎ））（１５００＜＝ｎ＜１６００）のキーを、コンテンツ情報を利用できる有効期間が例えば１００時間未満の場合に用いるようにしてもよい。すなわち、マスターキー生成部３０６９は例えば１時間毎にキーの対を生成し、ｎ＝１５００からｎ＝１５９９に順次記録して行く。指定された有効期間に応じて、例えば有効期間が最長の１００時間未満の場合（ＫＰ（１５９９ｎ）、Ｋｓ（１５９９））を記録した後は再び（ＫＰ（１５００）、Ｋｓ（１５００））を上書きし、以後これを繰り返す。

【０３２１】

このようなマスターキー（（ＫＰ（ｎ）、Ｋｓ（ｎ））（１５００＜＝ｎ＜１６００）のキー）を用いる場合、ライセンス情報の暗号化には、常に最新のＫＰ（ｎ）を用いる。ライセンス情報記録後、最長で９９時間までは、ＫＰ（ｎ）で暗号化されたライセンス情報は対応するＫｓ（ｎ）で復号されるが、１００時間以上の時間が経過すると、Ｋｓ（ｎ）

が失われてしまう（上書きにより変更されてしまう）為、このライセンス情報を復号する事はもはや不可能になる。これによって、高いセキュリティを確保する事が可能である。たとえ、何らかの方法でマスターキーＫｓ（ｎ）を読み取った者がいたとしても、このキーは特定の１時間の間に作成されたライセンス情報に対してのみ、有効である。

【０３２２】

以上の様に、マスターキー格納部３０６２がそれぞれ性質の異なる３種類のマスターキー（すなわち、全ての復号判定カードで共通の秘密鍵、各復号判定カードでユニークな秘密鍵、各復号判定カードで所定時間毎に更新される秘密鍵）を保持することによって、セキュリティと利便性のカスタマイズが可能となる。

【０３２３】

Ｋｍ（０）からＫｍ（９９９）にそれぞれ対応する暗号キーＫＭ（０）、…、ＫＭ（９９９）で暗号化されたライセンス情報は、どの復号判定カードによっても復号判定に使用することができる。しかし、万が一復号判定カードの内容が盗み取られた場合、コンテンツの保護が破綻してしまうと言うリスクが伴う。

【０３２４】

一方、公開マスターキーによる方法は、ライセンス情報更新の際、公開マスターキーをサーバーに送る必要がある。従って、利用者に余分な手間を強いる場合もある。

しかし、復号判定カードの内容が盗み読まれた場合にも、セキュリティの破綻は特定の復号判定カードに限定される。特に、上述の様な時変方式の公開マスターキーを使用した場合、セキュリティの破綻は時間的にも限定される。

（１－８）情報再生部

図９２は、図７７の情報再生部３００４の構成例を示したもので、認証部３０５１、復号部３０５２、デコーダ３０５３、Ｄ／Ａ変換部３０５４から構成されている。

【０３２５】

図９３に示すフローチャートを参照して図９２の情報再生部３００４の処理動作の概略を説明する。情報再生部３００４は例えばＭＰＥＧ２等の動画再生を行う。

【０３２６】

復号判定カード３００１から転送された暗号化されたコンテンツキー［Ｋｃ］Ｋ’Ｔは、情報再生部３００４の認証部３０５１に入力する。認証部３０５１は自らが生成した転送キーＫ’Ｔを用いて［Ｋｃ］Ｋ’Ｔを復号し、コンテンツキーＫｃを得る（ステップＳ３０８１）。

【０３２７】

一方、復号部３０５２には、メディア読取装置３００３でメディア３００２から読み取られたコンテンツキーＫｃで暗号化されたコンテンツ情報が入力する。復号部３０５２は、コンテンツキーＫｃでコンテンツ情報を復号しデコーダ３０５３に出力する（ステップＳ３０８２）。

【０３２８】

デコーダ３０５３は、圧縮の為に施されたコーディングを復元し、その結果得られた画像データ等をＤ／Ａ変換部３０５４に送る（ステップＳ３０８３）。

【０３２９】

Ｄ／Ａ変換部３０５４は、これをアナログ信号に変換し、所定の表示装置に出力する（ステップＳ３０８５）。

【０３３０】

図９４は、図９２の情報再生部３００４の認証部３０５１の構成例を示したものである。図９５に示すフローチャートを参照して認証部３０５１の処理動作について説明する。

【０３３１】

復号判定カード３００１から情報再生部３００４に転送された乱数Ｃは、認証部３０５１の入出力部３０５１ａに入力し、乱数格納部３０５１ｂに格納される（ステップＳ３０９１）。

【０３３２】

乱数発生部３０５１ｃは乱数Ｄを発生し、乱数格納部３０５１ｄに格納する（ステップＳ３０９２）。

【０３３３】

転送鍵生成部３０５１ｆは、乱数格納部３０５１ｂ、３０５１ｄからそれぞれ乱数Ｃ、乱数Ｄを読み出し、また、秘密鍵格納部３０５１ｅから鍵生成情報Ｋ’ｔを読み出して、転送キーＫ’Ｔを生成する（ステップＳ３０９３）。この生成された転送キーＫ’Ｔは転送鍵格納部３０５１ｇに格納される（ステップＳ３０９４）。

【０３３４】

乱数格納部３０５１ｄに格納された乱数Ｄは、また、入出力部３０５１ａを介して復号判定ユニット３００１へ転送される（ステップＳ３０９５）。

【０３３５】

復号判定カード３００１から情報再生部３００４に転送された暗号化されたコンテンツキー［Ｋｃ］Ｋ’Ｔは、認証部３０５１の入出力部３０５１ａに入力する。［Ｋｃ］Ｋ’Ｔは復号部３０５１ｈに出力される（ステップＳ３０９６）。復号部３０５１ｈは、転送鍵格納部３０５１ｇから転送キーＫ’Ｔを読み出して［Ｋｃ］Ｋ’Ｔを復号し、コンテンツキーＫｃを得る（ステップＳ３０９７）。コンテンツキーＫｃは情報再生部３００４内の復号部３０５２に出力される（ステップＳ３０９８）。

（１－９）他の情報再生部

図９６は、図７７の情報再生部３００４の他の構成例を示したもので、課金対象のコンテンツ情報がプログラムである場合を示している。この場合、課金対象のコンテンツ情報の少なくとも一部は、コンテンツキーＫｃにより暗号化されており、当該コンテンツキーＫｃがライセンス情報に含まれている。

【０３３６】

図９６において、図９２と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図９６において、図９２のデコーダ３０５３、Ｄ／Ａ変換部３０５４がプログラム実行部３０５５に置き換わり、プログラム実行部３０５５にてコンテンツ情報としてのプログラムが実行されるようになっている。情報再生部３００４にコンテンツキーＫｃと暗号化されたコンテンツ情報とが送られてくるまでの動作は、前述同様である。

【０３３７】

この場合の情報再生部３００４は、ＣＰＵ、メモリ等から構成される中央処理装置であっても良い。

（１－１０）

上記（１－１）～（１－９）は、図７７に示したように、情報再生装置が時計３００５を具備している場合である。勿論、復号判定カード３００１自身が時計を内蔵する場合も考えられる。この場合、復号判定カード３００１は時計の駆動用に電池を内蔵することになる。時計を復号判定カードに内蔵することのメリットは、図７９に示した時刻転送部３０１２と、時計との間の認証処理が不要になることである。

（２）

以下、図７６の情報流通システムについて説明する。

【０３３８】

この場合の情報再生装置の構成および処理動作は前述の図７５の場合とほぼ同様である。

【０３３９】

図７６の情報流通システムでは、リムーバブル情報蓄積メディアには、当初ライセンス情報は記録されておらず、コンテンツＩＤと暗号化されたコンテンツ情報とが記録されている。ライセンスの更新の際には、メディアと復号判定カードとをライセンス更新端末にセットする。更新端末はメディアからコンテンツＩＤ、復号判定カードから前述の公開マスターキーのうちの１つをそれぞれ読み取り、ライセンスサーバーに転送する。ライセンスサーバーは、取り扱いコンテンツのデータベースを具備しており、コンテンツＩＤをキーとしてデータベースを検索し、コンテンツキーを取得する。

【０３４０】

ライセンスサーバーは次いで、コンテンツキーを含む通常のライセンス情報を作成し、公開マスターキーによって暗号化して、更新端末に転送する。更新端末は、受け取った暗号化ライセンス情報をメディアに記録する。ライセンス情報記録後のメディアの再生は、図７５の情報流通システムの場合と同様である。

【０３４１】

次に、図７６の情報流通システムにおける、ライセンス更新端末とライセンスサーバーについてより詳細に説明する。

（２－１）ライセンス更新端末

ライセンス更新端末の構成を図９７に示す。

【０３４２】

ライセンス更新端末４０００は、挿入された復号判定カードから所定の情報を読み取るカードインターフェース（ＩＦ）４００１、挿入されたリムーバブル情報蓄積メディアから所定の情報を読み取るリムーバブル情報蓄積メディアドライブ４００２、所定の通信回線（例えば公衆回線、専用回線等）を介してライセンスサーバとの間の通信を行うための通信部４００３、例えば液晶表示パネル等から構成される表示部４００４、ユーザからの指示を入力するためのキーボード、タッチパネル等から構成されるキー入力部４００５から構成されている。

【０３４３】

図９８は、図９７に示したライセンス更新装置４０００の処理動作を示したフローチャートである。以下、図９８を参照してライセンス更新端末の処理動作について説明する。

【０３４４】

リムーバブル情報蓄積メディアドライブ４００２にリムーバブル情報蓄積メディアがセットされると当該メディアからそのメディアに記録されているコンテンツ情報の識別情報、すなわちコンテンツＩＤが読み取られ（ステップＳ４００１）、この読み取られたコンテンツＩＤと当該ライセンス更新端末の識別情報（更新端末ＩＤ）とが通信部４００３を介してライセンスサーバに送信される（ステップＳ４００２）。

【０３４５】

ライセンス更新端末からライセンスサーバーに対して送信される更新端末ＩＤは、ライセンスサーバーが更新端末ＩＤを更新情報と共に、更新ログとして保存する際に用いられる。また、コンテンツ利用料金の回収は、この更新ログに基づいて行われてもよい。

【０３４６】

コンテンツＩＤと更新と更新端末ＩＤとを受信したライセンスサーバでは、当該更新端末に課金メニュー、要求キー種別情報、認証キー番号Ｎを送信する（ステップＳ４００３）。

【０３４７】

ライセンスサーバから更新端末に送られてくる要求キー種別情報は、前述の３種類のマスターキーの指定するためのものである。前述したように、要求キー種別は、例えば次のようなものがある。

・　要求キー種別情報が「０」のとき…予め定められた復号用のマスターキー、すなわちＫｍ（０）、…、Ｋｍ（９９９）を指定

・　要求キーの種別情報が「１」のとき…ライセンス情報復号用の各判定カードでユニークなマスターキー、すなわちＫＰ（１０００）、…、ＫＰ（１４９９）を指定

・　要求キーの種別情報が「２」のとき…各判定カードで所定時間毎に更新される秘密鍵、ＫＰ（１５００）、…、ＫＰ（１５９９）を指定

ライセンスサーバからライセンス更新端末に送られてくる認証キー番号Ｎは、復号判定カードが転送の際の認証用に保持しているキーＫＮを指定する番号である。このキーＫＮによって暗号化されたマスターキーＫＰは、ライセンスサーバが保持するＫＮに対応する復号鍵Ｋ’Ｎによって復号される。ライセンスサーバは、この様にして得たキーＫＰを用いてライセンス情報を暗号化して、ライセンス更新端末に送信する。従って、（例えば、正当でない装置が復号判定カードに成りすまそうとした場合の様に）復号判定カードが正し

い認証キーＫＮを保持していない場合、リムーバブル情報記録メディアに記録されるライセンス情報は、ＫＰに対応する復号鍵Ｋｓによって復号することができない。かくして、正当でない復号判定カードは排除される。

【０３４８】

課金メニューは、コンテンツ情報の有効期間に応じた料金表で、この課金メニューから所望の有効期間を選択して料金の支払を行うようになっている。課金メニューは例えば、有効期間に対応する料金と、その有効期間を選択する際の識別番号とから構成されている。具体的には、有効期間が７日間のときの料金は２００円で識別番号は「１」、有効期間が３０日間のときの料金は５００円で識別番号は「２」、有効期限が無期限（譲渡）のとき料金は３０００円で識別番号「３」となる。

【０３４９】

なお、要求キー種別情報が「０」のとき、ライセンス更新端末はマスターキーＫＰをライセンスサーバに送る必要はない。何故なら、ライセンス情報が全ての復号判定カードに共通するキーで暗号化されて、ライセンスサーバから送られて来るからである。この場合、サーバから送られるライセンス情報にはＫｍの番号の指定が添えられている。この番号は暗号化されている必要は無い。

【０３５０】

更新端末とライセンスサーバとの間の通信回線が専用回線でない場合、情報セキュリティ対策として、ライセンスサーバの通信部４０２１と更新端末の通信部４００３とが通信を行う際に相互認証の手続きを行うことが望ましい。この場合、ライセンス更新に対する課金はライセンス更新端末を設置する店舗で行う。正当でないライセンス更新端末を排除しなければ、課金が正しく行われない可能性があるからである。また、ライセンス更新端末の設置者にとっても正当でないライセンスサーバに接続すると、不正なライセンス情報で利用者に課金してしまう危険が存在するからである。

【０３５１】

通信回線が専用回線で、通信先が信頼できる場合、相互認証は不要となる。なお、ライセンス更新端末からライセンスサーバへの接続にインターネットなどの一般回線が利用されるライセンス更新端末の通信部４００３は、ライセンスサーバとの通新記録を保存する様にしても良い。料金の回収はライセンスサーバの記録に基づいて行われるから、ライセンス更新端末側にも確認の為に記録を残しておく方が運用上好ましい。

【０３５２】

さて、ライセンス更新端末の通信部は４００３、ライセンスサーバから送信された情報のうち、課金メニューを表示部４００４で転送し、要求キー識別情報と認証キー番号ＮとをカードＩＦ４００１に転送する（ステップＳ４００４）。

【０３５３】

表示部４００４は課金メニューを提示して、ユーザに有効期間の識別番号の選択を促す。一方、カードＩＦ４００１は、要求キー識別情報と認証キー番号とを復号判定カードへ転送する。復号判定カードでは、これらの情報を受けて、要求キー識別情報に対応したマスターキーＫＰ（複数のＫＰのうちの適当な１つ）を認証キー番号にて指定された認証キーＫＮで暗号化したもの、すなわち［ＫＰ］ＫＮをカードＩＦ４００１へ転送する。その際、マスターキーの識別情報も転送するようにしてもよい。

【０３５４】

通信部４００３には、カードＩＦから転送された［ＫＰ］ＫＮと、表示部４００４を介してユーザにより指定された課金メニュー中の有効期間の識別番号とをライセンスサーバに送信する（ステップＳ４００５～ステップＳ４００７）。

【０３５５】

これを受けてライセンスサーバからは、少なくとも、当該更新端末から通知されたマスターキーＫＰにて暗号化されたライセンス情報、すなわち［ライセンス情報］ＫＰが送信されて、更新端末の通信部４００３が受信する（ステップＳ４００８）。

【０３５６】

［ライセンス情報］ＫＰは、リムーバブル情報蓄積メディアドライブ４００２にてそこにセットされているメディアに記録される（ステップＳ４００９）。なお、メディアにはライセンスサーバから送信された［ライセンス情報］ＫＰとマスターキーの識別情報とが記録されてもよい。

（２－２）復号判定カード

図９９は、復号判定カードの３０１５のライセンス更新装置とのインターフェースを司る復号判定カード３０１５の要部、すなわち、更新インターフェース（ＩＦ）３０１５の構成例を示したものである。

【０３５７】

以下、図１００に示すフローチャートを参照して図９９の各構成部の処理動作について説明する。

【０３５８】

図９８のステップＳ４００４で更新端末のカードＩＦ４００１から復号判定カード３０１５に対し転送された要求キー識別情報と認証キー番号Ｎとは入出力部４０１１に入力する（ステップＳ４０１１）。

【０３５９】

入出力部４０１１は、要求キー識別情報をマスターキー選択部３０６１へ転送し、認証キー番号Ｎを認証キー選択部４０１４へ転送する（ステップＳ４０１２）。

【０３６０】

マスターキー選択部３０６１は、マスターキー格納部３０６２を検索して、要求キー識別情報に適合するマスターキーＫＰを選択し、暗号部４０１２へ転送する（ステップＳ４０１３）。

【０３６１】

認証キー選択部４０１４は、認証キー格納部４０１３を検索して認証キー番号Ｎの認証キーＫＮを選択し、暗号部４０１２へ転送する（ステップＳ４０１４）。

【０３６２】

暗号化部４０１２は、マスターキーＫＰを認証キーＫＮで暗号化し、［ＫＰ］ＫＮを生成する（ステップＳ４０１５）。［ＫＰ］ＫＮは入出力部４０１１を介してライセンス更新装置へ出力される（ステップＳ４０１６）。

（２－３）ライセンスサーバ

図１０１は、ライセンスサーバの構成例を示したものである。

【０３６３】

コンテンツ情報データベース（ＤＢ）４０２４には、例えば、コンテンツＩＤに対応させて次の様な情報が格納されている。

【０３６４】

・コンテンツキー
・課金メニュー
・要求キー種別

以下、図１０１のライセンスサーバ４００１の各構成部の処理動作について図１０２に示すフローチャートを参照して説明する。

【０３６５】

図９８のステップＳ４００２でライセンス更新端末から送信されたコンテンツＩＤと更新端末ＩＤは、通信部４０２１にて受信され、応答部４０２２へ転送される（ステップＳ４０２１）。

【０３６６】

応答部４０２２はコンテンツＩＤをコンテンツ情報検索部４０２３へ転送し（ステップＳ４０２２）、コンテンツ情報検索部４０２３は、コンテンツＩＤを基にそれに対応するコンテンツキー、課金メニュー、要求キー種別を読み出し、これらの情報を応答部４０２２へ転送する（ステップＳ４０２３）。

【０３６７】

一方、応答部４０２２は、認証キー番号Ｎを生成する（ステップＳ４０２４）。例えば、予め定められた複数の認証キー番号のうちから１つを選択するようにしてもよい。そして、コンテンツキー以外の情報、すなわち、課金メニュー、要求キー種別情報、認証キー番号Ｎを通信部４０２１を介してライセンス更新端末に送信する（ステップＳ４０２５）。

【０３６８】

図９８のステップＳ４００７で更新端末から送信された［ＫＰ］ＫＮ、課金メニュー中の所望の有効期間の識別番号は、通信部４０２１で受信され、これらは応答部４０２２へ転送される（ステップＳ４０２６）。

【０３６９】

応答部４０２２では、先に生成された認証キー番号Ｎに対応する復号鍵ＫＮ’で［ＫＰ］ＫＮを復号し、マスターキーＫＰを得る（ステップＳ４０２７）。

【０３７０】

応答部４０２２にて生成されたライセンス情報は、暗号化部４０２５でマスターキーＫＰを用いて暗号化され（［ライセンス情報］ＫＰを生成し）、［ライセンス情報］ＫＰは通信部４０２１を介してライセンス更新装置に送信される（ステップＳ４０２８～ステップＳ４０２９）。

【０３７１】

応答部４０２２は、更新記録データベース（ＤＢ）４０２６に、ステップＳ４０２１にて受信した更新端末ＩＤに対応させて、ライセンスの更新履歴情報を記録する（ステップＳ４０３０）。

（３）ユーザ端末から電子決済を利用してライセンス更新を行う場合の情報流通システム

図１０３に電子決済を利用してライセンスを更新する場合のユーザ端末、ライセンスサーバ４１０１、電子決済装置４１０２からなるシステム構成の一例を示したもので、ユーザ端末がネットワーク経由の電子決済によって、課金処理を行うようになっている。

【０３７２】

ユーザ端末は、少なくともライセンス更新装置４１０３を具備するとともに、復号判定カード３００１とリムーバブル情報記憶メディア４０３１とが装着された、例えばパーソナルコンピュータで構成されるものであってもよい。

【０３７３】

図１０４は、ユーザ端末に具備されたライセンス更新装置４１０３の構成例を示したもので、ＣＰＵ等から構成される制御部４０４４が通信部４０４１、リムーバブル情報記録メディアＩＦ４０４２、復号判定カードＩＦ４０４３、表示部４０４５、入力部４０４６の各構成部を制御して、ライセンスを更新するための処理を実行するようになっている。

【０３７４】

図１０５はライセンスサーバ４１０１の構成例を示したもので、制御部４０５３が通信部４０５１、復号部４０５２、課金整理番号発行部４０５４、課金処理部４０５５、ライセンス情報生成部４０５６の各構成部を制御してライセンスを更新するための処理を実行するようになっている。

【０３７５】

図１０６は、全てのライセンス判定カードに共通の（従って、全てのユーザ端末に共通の）マスターキー（例えばＫｍ（０）、…、Ｋｍ（９９９）のうちの１つ）によってライセンス情報が暗号化されている場合を例にとり、図１０３に示したシステム全体の処理動作を示したフローチャートである。

【０３７６】

以下、図１０６に示したフローチャートを参照して、ライセンス更新装置４１０３、ライセンスサーバ４１０１の各構成部の処理動作を説明する。

【０３７７】

なお、メディア４０３１にはコンテンツ情報とライセンス情報とが記録されており、ライセンス情報には、例えば該コンテンツ情報の利用の可否を判定するための利用条件やコンテンツＩＤ、その他の情報が含まれているものとする。

【０３７８】
ライセンス更新装置４１０３のリムーバブル情報記録メディアインターフェース（ＩＦ）４０４２は、ユーザ端末にセットされたメディアからライセンス情報を読取り、それを復号判定カードインターフェース（ＩＦ）４０４３を介して復号判定カード３００１へ出力する（ステップＳ４０４１）。
【０３７９】
復号判定カード３００１では、例えば、入力されたライセンス情報に基づき所定の処理（例えば、第２の実施形態で説明した復号ユニットＡ等の処理動作参照）を行い、その結果、ライセンスの更新を行う場合、ライセンスの更新情報（例えば、復号ユニットＡの場合、図５６に示したような更新情報）を出力する。
【０３８０】
復号判定カードＩＦ４０４３は、次に、復号判定カード３００１からライセンスサーバＩＤを読み取る（ステップＳ４０４２）。なお、ライセンスサーバＩＤは更新情報に含まれていてもよい。
【０３８１】
ライセンスサーバＩＤは、ライセンスサーバを特定するための識別情報である。
【０３８２】
ライセンス更新装置４１０３は、通信部４０４１を介してライセンスサーバＩＤにて特定されるライセンスサーバにアクセスしてライセンス情報を更新するための更新情報を送信する（ステップＳ４０４３）。
【０３８３】
ライセンスサーバ４１０１の通信部４０５１が、ライセンス更新装置４１０３から送信された更新情報を受信すると、更新情報に含まれるコンテンツＩＤを基に課金データベース（ＤＢ）４０５８を検索して、少なくとも課金メニューを読み出し（必要に応じて要求キー種別情報、認証キー番号Ｎ等）、さらに、課金整理番号発行部４０５４で課金整理番号を発行し、少なくとも課金メニューと課金整理番号（以下、データ群Ａと呼ぶことがある）を通信部４０５１を介してライセンス更新装置４１０３に送信する（ステップＳ４０４４）。
【０３８４】
ライセンスサーバから発行される課金整理番号は、ライセンスサーバがトランザクション毎に適当に割り付ける番号である。課金整理番号は、後述する様に、課金確認の為に用いられる。
【０３８５】
ライセンスサーバは通常、複数のユーザ、すなわちライセンス更新装置からのライセンス更新要求を処理する。従って、回線接続時間は可能な限り短くする事が好ましい。その為、ライセンス更新装置は、ライセンスサーバとの回線を適宜切断する。例えば、ライセンス更新装置の通信部４０４１には、ライセンスサーバからの応答待ち時間Ｔｗが予め定められていて、この時間内にライセンスサーバから応答がない場合は、回線を切断するようにしてもよい。また、複数ｎライセンス更新装置のそれぞれからのライセンス更新要求を区別する為に、ライセンスサーバは課金整理番号に基づいて、ライセンス情報の管理を行う必要がある。
データ群Ａを受信したライセンス更新装置４１０３は、課金メニューを表示部４０４５に提示し（ステップＳ４０４５）、ユーザにより所望の有効期間の識別番号が選択されたら（ステップＳ４０４６）、ライセンス更新装置４１０３の通信部４０４１は電子決済装置４１０２にアクセスし、少なくとも課金整理番号とライセンスサーバＩＤと選択された有効期間の識別番号とそれに対応する料金の支払要求を行う（ステップＳ４０４７）。
【０３８６】
電子決済装置４１０２は、ユーザからの要求に応じて所定の支払処理を行い、処理が成功すればライセンスサーバＩＤにて指定されるライセンスサーバ４１０１に、例えば有効期間の識別番号と決済金額と課金整理番号を支払証明として送信して支払処理の成功を通知

する。また、支払要求元のライセンス更新装置４１０３へも例えば有効期間の識別番号と決済金額と課金整理番号とを支払証明として送信する（ステップＳ４０４８～ステップＳ４０５０）。ライセンス更新装置４１０３では、決済金額と課金整理番号を受信すると、ライセンスサーバＩＤにて特定されるライセンスサーバにアクセスして、少なくとも、ステップＳ４０４６で選択された有効期間の識別番号と上記決済金額と課金整理番号とを支払証明として送信する（ステップＳ４０５１）。

【０３８７】

ライセンスサーバ４１０１の通信部４０５１にて受信された、電子決済装置４１０２から送信された支払証明と、ステップＳ４０５１にてライセンス更新装置４１０３から送信された支払証明とは、その課金整理番号に対応させて課金処理データベース（ＤＢ）４０５７に記録される。

【０３８８】

課金処理ＤＢ４０５７には、例えば、次のような情報が各課金整理番号に対応させて記憶するようになっている。

【０３８９】

・ライセンス更新端末のＩＤ
・コンテンツキー
・電子決済装置からの支払証明（有効期間の識別番号、決済金額、課金整理番号）
・ライセンス更新装置からの支払証明（有効期間の識別番号、決済金額、課金整理番号）

ラインセンスサーバ４１０１では、電子決済装置４１０２、ライセンス更新装置４１０３とからそれぞれ支払証明を受信すると、課金処理ＤＢ４０５７に記録し、課金処理部４０５５にて双方の支払証明にある決済金額と識別番号とが一致するか否かを確認する（ステップＳ４０５２）。一致していた場合に限り適正な支払が行われたと判断できる。このような支払証明の確認処理と並行して、ライセンスサーバ４１０１のライセンス情報生成部４０５６では、ステップＳ４０４３にてライセンス更新装置４１０３から送信されたライセンスの更新情報と、コンテンツ情報ＤＢ４０２４から検索されたコンテンツＩＤに対応するコンテンツキーとに基づき、少なくともライセンス情報中の利用条件、コンテンツキー等を変更する（ライセンス情報を更新する）。

【０３９０】

ライセンス情報には、例えば、次の様な情報が含まれている。

・コンテンツＩＤ
・暗号化されたコンテンツ情報を復号するコンテンツキー
・少なくとも有効期限を含むコンテンツ情報の利用条件
・ライセンス情報の作成時刻
・更新サーバＩＤ
・課金整理番号

ここで、更新サーバーＩＤは、今回ライセンスの更新を行ったライセンスサーバを特定する識別情報である。更新サーバＩＤによって、必要に応じて、ライセンス情報から更新を行ったサーバーを特定する事が可能となる。

【０３９１】

ステップＳ４０５３で、適正な支払が行われたことが確認されると、ライセンスサーバ４１０１は、通信部４０５１を介して更新されたライセンス情報をライセンス更新元のライセンス更新装置４１０３に送信する（ステップＳ４０５４）。

【０３９２】

更新されたライセンス情報を受信したライセンス更新装置４１０３では、リムーバブル情報記録メディアＩＦ４０４２を介してメディア４０３１に該更新されたライセンス情報を記録する（ステップＳ４０５５）。

【０３９３】

（第４の実施形態）

図１０７は、第４の実施形態に係る情報再生システムの全体の構成例を示したもので、例

えば、図５３、図７５、図７６、後述する図１２２に示したような情報流通システムでユーザにより用いられるものである。コンテンツ情報は、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＯＭ等の記録媒体（情報メディア）に記録されている。予め定められた条件下における当該コンテンツ情報の利用（再生および視聴）権をライセンスといい、このライセンスを購入することにより、ユーザにライセンス情報が与えられる。当該コンテンツ情報の再生を可能にするライセンス情報は、コンテンツ情報の記録されている記録媒体に一緒に記録されていてもよいし、コンテンツ情報とは別個に、その他の記録媒体あるいはメモリおよび演算機能を有するＩＣカード等に記録されていて、コンテンツ情報とは別個に読み取られ、図１０７に示す情報再生装置に入力されるものであってもよい。あるいは、放送やインターネット等を通じて配信されるものであってもよい。

【０３９４】

図１０７において、情報再生システムは、主にデジタルコンテンツである暗号化コンテンツ情報をＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ等の情報メディアから読み取る情報メディアドライバ７００１、暗号化コンテンツに対応するライセンス情報に基づいて当該ライセンスが有効かどうかのチェックを行い、有効ならば当該コンテンツ情報を利用するためのコンテンツ復号鍵を出力する情報再生装置７００、情報再生装置７０００から出力される復号鍵で暗号化コンテンツを復号し、再生する、ＤＶＤプレーヤ、ビデオ再生装置などの情報利用装置７００２から構成される。

【０３９５】

ライセンス料の着実な徴収のためデジタルコンテンツは予め暗号化されていると仮定している。本実施形態で用いるコンテンツ情報の構成例を図１１３に示す。即ち、コンテンツは暗号化部分と未暗号化部分に分かれ、暗号化部分には暗号化コンテンツが、未暗号化部分にはコンテンツＩＤが記録される。コンテンツＩＤはコンテンツとそのライセンス情報のリンクを取るためのものである。

【０３９６】

図１１４は、ライセンス情報の構成例を示したもので、暗号化コンテンツを解除する復号鍵（以下コンテンツ復号鍵という）と、利用期限などのライセンス利用条件と、当該コンテンツのＩＤと、ライセンス認証情報とがが含まれている。

ライセンス認証情報とは、暗号化されたライセンス情報が正確に復号されたか否かをチェックするための定められたコードである。例えば、４バイトコードであれば１６進数で「ａ５ｆｅ４７８ｅ１６０ｅ３２５ｆ」と表されるようなコードである。これは、予めライセンス生成装置、ライセンス更新装置及びライセンス判定ユニットの間で定めておくべき情報である。

【０３９７】

ライセンス情報は、その全体を予め定められた公開鍵で暗号化されている。このライセンス情報の復号は、情報再生装置７０００に具備されるライセンス判定ユニット７００８内で当該ユニット内に存在する秘密鍵を用いて行い、復号されたライセンス情報に基づいて利用条件のチェックを行う。利用条件として、例えば利用期限と利用回数とがある。利用条件として利用期限を採用することにより、利用期限後には視聴できなくなり、また、コンテンツと、そのコンテンツを復号するために必要なライセンス情報とをまるごと不正コピーしたとしても利用期限後には使えなくなるので海賊版の流通を実質的に意味のないものとすることができる。

【０３９８】

だが、利用期限を定めた場合、その利用条件のチェックのための現在時刻（以下、時刻とは日付けおよび時刻を意味するものとする）を計時する時計の管理を着実に行わないと、利用期限自体無意味なものとなる。例えば、１２月１５日に１週間分のライセンスとして１２月２２日までの利用期限を有するライセンス情報を取得したとしても、ライセンス判定ユニット７００８が参照する時計が６月１０日を示していたら半年分のライセンスになってしまうのである。特に、このようなことは時計が、ユーザに調整可能であれば、ユーザによって時計を都合良く調整される可能性があるので十分起こり得ることである。

【０３９９】
そこで、本実施形態では、この点を改善し、時計を都合良く調整した場合でも利用期限を遵守させる枠組を提供できる情報再生装置について説明する。すなわち、ライセンス情報の復号鍵を一定時間毎に予め定められたアルゴリズムで生成し、それ以前の復号鍵と置き換え、ライセンス生成装置やライセンス更新装置においても同じタイミングで対応するライセンス情報の暗号鍵を生成することによって、時計の時刻がライセンス生成装置もしくはライセンス更新装置のそれから著しくずれている場合は、新たに取得したライセンス情報が復号できなくなる。従って、少なくとも新しいコンテンツを視聴したい場合は時計の時刻を正確に合わせる必要があるのである。このようにライセンス情報の復号鍵を変化させることによって間接的に時計を正しい状態にするというのが本実施形態の主旨である。なお、図１０７において、現在時刻を計時するための時計７００８ｈ（図１０８参照）は、ライセンス判定ユニット７００８の内部に設けられているが（この場合、ライセンス判定ユニット７００８を例えば１つのＩＣチップで構成し、ユーザにより計時時刻が調整されることがないようにハードウエア的に保護する構成が容易に行えるが）、時計７００８ｈの計時時刻はユーザにより調整可能であってもよい。

【０４００】
次に、図１０９～図１１０に示すフローチャートを参照して、図１０７の情報再生装置の処理動作および図１０８に示すような構成のライセンス判定ユニット７００８の処理動作について説明する。

【０４０１】
情報メディアドライバ７００１から読み取られた図１１３のようなコンテンツ情報は、データ分離部７００７でコンテンツＩＤと暗号化コンテンツに分離される（ステップＳ７００１～ステップＳ７００２）。暗号化コンテンツは情報利用装置７００２に送られ（ステップＳ７００３）、ライセンス判定ユニット７００８から出力されるコンテンツ復号鍵を待つ。

【０４０２】
一方、コンテンツＩＤはライセンス情報検索部７００６に送られる。ライセンス情報検索部７００６は、ライセンス情報データベース（ＤＢ）７００４から当該コンテンツＩＤを持ったライセンス情報を検索する（ステップＳ７００４）。
ライセンス情報ＤＢ７００４に記憶されているライセンス情報は、図１１５に示すように、少なくともコンテンツＩＤを含む未暗号化部を暗号化ライセンス情報に付加されていて、コンテンツＩＤで該コンテンツに対応するライセンス情報が検索できるようになっている。検索されたライセンス情報はライセンス判定ユニット７００８へ送られる（ステップＳ７００５～ステップＳ７００６）。

【０４０３】
図１０８は、ライセンス判定ユニット７００８の構成例を示したものである。ライセンス情報検索部７００６で検索されたライセンス情報は、ライセンス情報入力部７００８ａに入力し、復号部７００８ｂへ転送される。

【０４０４】
復号部７００８ｂでは、復号鍵格納部７００８ｅに格納されているライセンス情報復号鍵を使ってライセンス情報を復号する（ステップＳ７００７～ステップＳ７００８）。

【０４０５】
復号されたライセンス情報はライセンス情報整合性確認部７００８ｃでライセンス認証情報を使ってライセンス情報が正しく復号されたことを確認する（ステップＳ７００９）。すなわち、ライセンス情報が復号された際、ライセンス情報のデータ中の予め定められた場所にライセンス認証情報があるかどうかをチェックして、もしあればライセンス情報を正しく復号できたと判定する。もちろん適切な復号鍵で復号していれば通常このコードはでたらめなものになる。もし、ライセンス情報が正しく復号されていないと判定した場合、ライセンス情報検索部７００６へライセンス情報の次候補の検索を要請する。ライセンス情報検索部７００８ではこれを受けてライセンス情報ＤＢ７００４を検索し、当該コン

テンツＩＤを持つ次のライセンス情報を抽出して、ライセンス判定ユニット７００８に送る。もし、ライセンス情報検索部７００６でライセンス情報の次候補が検索できなかった場合、図１１０のステップＳ７０２１へ進み、表示部７０１１に、例えば「ライセンス情報が無効であるか、参照時計の時刻が間違っています。現在の参照時計の時刻はＹＹＹＹ年ＨＨ時ＭＭ分です。時刻を確認した上で、ライセンスの更新を行ってください。」という旨のメッセージの表示を要請する（図１１０のステップＳ７０２１）。これを見てユーザは現在の時刻を確認し、時刻が著しくずれていた場合は修正する。

【０４０６】

復号鍵生成部７００８ｆは、ライセンスを発行するライセンス更新装置、ライセンス作成装置とともに一定時間毎に鍵を新たに生成し、復号鍵格納部７００８ｅに格納する。そのため、ライセンス判定ユニット７００８の時計７００８ｈが実際の時刻と著しくずれている場合、ライセンス判定ユニット７００８で生成される復号鍵とライセンス更新装置もしくはライセンス生成装置で生成される暗号鍵との整合がとれず、従って、利用条件が有効なライセンス情報であっても復号できない。このため、上記表示メッセージのように、ユーザに時計７００８ｈの時刻確認を求める必要がある。その後、ユーザの要求に応じてライセンスの更新を行うようにしてもよい。

【０４０７】

さて、図１０９のステップＳ７０１０で、ライセンス情報整合性確認部７００８ｃでライセンス情報が正しく復号されたと判定された場合、ライセンス情報は利用条件判定部７００８ｄへ送られ、引続き利用条件の判定が行われる。利用条件として利用期限を用いているので、利用条件の判定は時計参照部７００８ｇを介して、ライセンス判定ユニット７００８の内部、場合によっては外部にある時計７００８ｈの時刻を参照して、該時刻が利用期限内であるか否かを判定する（ステップＳ７０１１）。利用条件を満たしていると判定されれば（ステップＳ７０１２）、コンテンツ復号鍵が情報利用装置７００２に出力され（ステップＳ７０１３）、情報利用装置７００２では、これを使って別途送られた暗号化コンテンツを復号し、再生利用する（ステップＳ７０１４）。

【０４０８】

一方、ステップＳ７０１２でライセンスの利用条件が満たされていなかった場合は、その旨と少なくとも当該ライセンス情報とをライセンス情報検索部７００６へ転送し、図１１０のステップＳ７０２１へ進み、ユーザからの要求に応じて、当該ライセンスの更新を行うようにしてもよい。

【０４０９】

ライセンスの更新は、後に詳しく述べるような手続きで、図１０７のライセンス更新指示部７００５、希望利用条件入力部７０１０、表示部７０１１などを通じて、図１１６に示したような、少なくともコンテンツＩＤと希望利用条件を含むライセンス更新情報を作成し、作成されたライセンス更新情報を例えばインターネットのような所定のネットワークを介してライセンス更新装置に送り、ライセンス情報の更新を行なう。

【０４１０】

図１１０に示すフローチャートは、ライセンス情報の更新処理動作を示したもので、ライセンス情報検索部７００６では、表示部７０１１に「ライセンス情報が無効であるか、参照時計の時刻が間違っています。現在の参照時計の時刻はＹＹＹＹ年ＨＨ時ＭＭ分です。時刻を確認した上で、ライセンスの更新を行ってください。」という主旨のメッセージを表示した後（ステップＳ７０２１）、少なくともユーザがライセンス更新をするか否かの指示入力を行うための適切なインターフェースを具備したライセンス更新指示部７００５を起動する。ユーザは、（例えば、時計７００８ｈの時刻の確認等を行った後）、このインターフェースを介してライセンス更新を行う旨の指示入力を行ったとする。ライセンス更新指示部７００５は、それをライセンス情報検索部７００６に送り、ライセンス情報検索部７００６は当該コンテンツＩＤをライセンス更新部７００９に送る（ステップＳ７０２２～７０２４）。

【０４１１】

ライセンス更新部７００９は、希望利用条件入力部７０１０を起動し、希望利用条件入力部７０１０の適切なインターフェースを介して入力された希望利用条件と、ライセンス情報検索部７００６から送られてきたコンテンツＩＤとを用いて、図１１６に示したようなライセンス更新情報を作成し（ステップＳ７０２５～ステップＳ７０２７）、当該ライセンス更新情報を所定のネットワークを介してライセンス情報更新装置に送る。

【０４１２】

ステップＳ７０２４で、ユーザがライセンス更新をしない場合（すなわち、ユーザがライセンス更新指示部７００５を介してライセンスを更新しない旨の指示入力を行った場合）、ライセンス情報検索部７００６では、コンテンツＩＤを消去し、処理が終了する。

【０４１３】

更新されたライセンス情報は、図１１１に示すように、ＩＣカード等を介して、あるいは、インターネット等の所定のネットワークを介してライセンス格納部７００３に入力され、図１１５に示したようなデータ形式に変換されて、ライセンス情報ＤＢ７００４に記憶される。

【０４１４】

なお、ライセンス判定ユニット７００８でライセンスが無効と判定された場合（図１０９のステップＳ７００５、ステップＳ７０１０、ステップＳ７０１２）には、そのまま処理を中断（再生を中止）するようにしてもよい。この場合は、ライセンス更新指示部７００５、表示部７０１１、ライセンス更新部７００９、希望条件入力部７０１０は不要となり、ライセンス更新装置と通信を行う機能も不要となり、構成も簡略となる。ライセンスを更新する際は、ユーザが例えばＩＣカードをもってライセンス更新を行う代理店等に赴き、所定の料金を支払い、利用条件等の更新された新たなライセンス情報を該ＩＣカードへ書き込んでもらう。そして、該ＩＣカードを持ち帰り、再び図１０７の情報再生装置へ挿入して、該更新されたライセンス情報を読み込ませて、ライセンス格納部７００３を介してライセンス情報ＤＢ７００４へ格納する。

【０４１５】

次に、ライセンス情報の復号鍵の生成処理動作について、図１１２に示すフローチャートを参照して説明する。

【０４１６】

ライセンス判定ユニット７００８の復号鍵生成部７００８ｆは、時計参照部７０８８ｇを介して時計７００８ｈを参照し、予め定められた時刻になったら復号鍵の生成を開始し（ステップＳ７０４１～ステップＳ７０４２）、生成された復号鍵は、復号鍵格納部７００８ｅに格納する（ステップＳ７０４３～ステップＳ７０４４）。復号鍵の生成はライセンス生成装置及びライセンス更新装置と同期して行わなくてはいけないものであり、例えば一週間に１度、毎週月曜日の午後１５：００というように決まった時間に更新する。また、その主旨からライセンス生成装置やライセンス更新装置と同じ鍵を作らなければならない。このため、例えば時刻をシードとした乱数生成器での鍵生成が考えられる。即ち、１９９７年１２月１５日に変更する場合は数字「１９９７１２１５」をシードとして、例えば復号鍵生成部７００８ｆに具備された乱数生成器の出力を復号鍵とするのである。勿論、ライセンス生成装置及びライセンス更新装置でも同じ方式でライセンス情報の暗号鍵生成する。

【０４１７】

以上は、共通鍵方式の場合の共通鍵を作る方式であるが、ライセンス判定ユニット７００８が公開鍵暗号を採用している場合もある。この場合は、前述の復号ユニットＡの鍵生成部２００６の場合の説明と同様に、例えばＲＳＡ暗号の鍵生成のアルゴリズムを用いて、復号鍵（秘密鍵）を生成すればよい。

【０４１８】

以上によって一定時間毎にライセンス生成装置とライセンス更新装置及びライセンス判定ユニット７００８の双方で復号鍵が変更できる仕組みができる。このため、ライセンス判定ユニット７００８を含む情報再生装置内の時計７００８ｈをユーザの操作によって改変

されても、新たに取得したライセンス情報は復号できなくなることから、時計の改変は多くの場合防止できる。

【０４１９】

なお、このような特徴から、時計７００８ｈがユーザの操作によって改変可能かどうかはあまり問題ではなくなる。

【０４２０】

また、鍵生成のプロセスにおいても、鍵生成の開始指示をを復号鍵生成部７００８ｆ自身が出すのではなく、時計参照部７００８ｇもしくは時計７００８ｈ自身が出すことも考えられる。この場合、復号鍵生成部７００８ｆが主導して復号鍵を生成するよりも、より正確な時刻に鍵生成が行える。

【０４２１】

さらに、本実施形態では、１つのコンテンツに対応したライセンスを検索したら、その有効判定（有効期限のチェック）を行ない、有効なら復号鍵を出力する。しかし、無効な場合、他のライセンス情報を検索せず、ライセンスが失効したか、参照時計が間違っている旨の表示を行うことになっている。これは当該コンテンツに対応したライセンス情報が１つのみと暗黙に仮定しているためである。しかし、例えば２週間分のライセンスを購入・販売する際、ライセンス情報を１週間毎に分離する場合もある。更に期間限定のライセンス以外に回数限定のライセンスを販売し、同じコンテンツに関してこれらが共存する場合もある。このような時は、存在するライセンス情報を全て検索し、ユーザにとって最も有利なライセンスを利用するように構成することも可能である。

【０４２２】

例えば、期間限定ライセンスの方を回数制限ライセンスよりも優先することによって、期間限定のライセンスがあるうちは回数限定のライセンスを使わなくてもすむので、ユーザにとっては有利である。この場合、ライセンス情報ＤＢ７００４に記憶されるライセンス情報は、図１１７に示すように、未暗号化部にはコンテンツＩＤの他に期間限定のライセンスかあるいは回数限定のライセンスかを識別するための情報が含まれていることが望ましい。

【０４２３】

ライセンスを選択する際の優先順位は、ユーザ自身で指定できるようにしてもよい。例えば、ライセンス情報検索部７００６が表示部７０１１に、期間限定のライセンスと回数限定のライセンスにいずれを優先するかをユーザに選択させるためのメニュー画面を表示してもよい。

【０４２４】

また、ライセンス情報検索部７００６は、最優先のライセンス情報が出現すればライセンス情報を全て検索しなくても、その時点で検索を終了するようにしてもよい。

【０４２５】

図１１８は、図１０７に示した情報再生装置７０００の他の構成例を示したもので、コンテンツ情報は、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＯＭ等の記録媒体（情報メディア）に記録され、ライセンス情報は、放送にて配信されるものとする。

【０４２６】

図１１８の情報再生装置では、放送配信される暗号化ライセンス情報の復号鍵を放送波に含まれるシードを基に生成することを特徴とし、その結果、復号鍵の生成を前述の時計７００８ｈを利用することなしに行うことができる。

【０４２７】

なお、図１１８において、図１０７と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図１１８に示す構成では、暗号化ライセンス情報が放送波によって送られ、その放送波には暗号化ライセンス情報の復号鍵を生成するためのシード情報が混在しているため、当該放送波を受信し、ディジタル信号に変換するためのライセンス情報受信部８００１と、ここで受信された放送波から暗号化ライセンス情報とシード情報とを分離するためのライセンス分離部８００２とを具備し、ライセンス判定ユニット８０

０９では、放送波にて送られていたシード情報に基づき復号鍵を生成するようになっている。

【０４２８】

図１２１は、ライセンス情報受信部８００１で受信される放送波のデータ構造の一例を示したものである。ライセンス情報とシード情報のそれぞれの先頭には、ライセンス情報とシード情報とを識別するための固定長の識別情報が付加されている。

【０４２９】

図１１９は、図１１８のライセンス判定ユニット８００９の構成例を示したものである。なお、図１１９において、図１０８と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図１１９に示すライセンス判定ユニット８００９では、ライセンス分離部８００２から出力されたシード情報が入力する復号鍵生成シード入力部８００９ｇをさらに具備し、復号鍵生成部８００９ｆでは、シード情報から復号鍵を生成するようになっている。

【０４３０】

次に、図１２０に示すフローチャートを参照して、受信した放送波から、暗号化ライセンス情報と復号鍵のシード情報を分離して復号鍵を生成するまでの動作について説明する。

【０４３１】

ライセンス情報受信部８００１では、放送波を受信し、図１２１に示すように受信データを得ると、その受信データを一旦ライセンス分離部８００２へ送り、識別情報を用いてライセンス情報とシード情報とに分解する（ステップＳ８００１～ステップＳ８００２）。

【０４３２】

受信データがライセンス情報であった場合、それをライセンス格納部７００３に送る（ステップＳ８００３～ステップＳ８００４）。ライセンス格納部７００３では、ライセンス情報を図１１５に示したようにコンテンツＩＤを付加して、ライセンスＤＢ７００４に格納する。一方、受信データがシード情報であった場合、当該シード情報をライセンス判定ユニットに送る（ステップＳ８００５）。ライセンス判定ユニットでは、これを、復号鍵生成シード入力部８００９ｇで受け、復号鍵生成部８００９ｆに送り、新たな復号鍵を生成する（ステップＳ８００６）。復号鍵生成部８００９ｆでは、例えば、シード情報から第４の実施形態と同様、共通鍵方式、公開鍵方式のいずれをもちいてもよい。生成された復号鍵は復号鍵格納部８００９ｅに格納される。

【０４３３】

ライセンス判定やライセンス更新の処理動作は、図１０９～図１１０と同様である。

【０４３４】

放送によってライセンス情報を配信する場合、ライセンスを全ての情報再生装置（受信端末）に送ったのでは、同じ仕様の受信端末を持った全ての人が視聴可能となってしまうので、ライセンスの管理をしているとは言えない。そのため、ライセンス情報を受信端末毎に与える必要があり、ライセンス情報の中に受信端末ＩＤを入れ、当該ＩＤを持つ受信端末以外の受信端末は受信できないようにする必要がある。そのため受信端末では、自分宛のライセンス情報のみを選別受信できるように、放送配信されるライセンス情報識別情報中に各受信端末を識別するための識別情報（受信端末ＩＤ）が含まれていることが望ましい。ここで、ライセンス情報識別情報中の受信端末ＩＤを有効端末ＩＤと呼ぶ。

【０４３５】

各受信端末、すなわち、図１１８に示したような情報再生装置のライセンス分離部８００２には、予め固有の受信端末ＩＤが記録されている。そして、図１２１に示したような受信データからライセンス情報を分離する際に、ライセンス情報識別情報に含まれる有効端末ＩＤと、自身のもつ受信端末ＩＤとを比較し、一致したときのみ当該ライセンス情報を取り込むようにする。あるいは、一旦全てのライセンス情報を所定のメモリに記憶しておいてから、そのメモリに記憶されたライセンス情報識別情報中の有効端末ＩＤと受信端末ＩＤとを比較して、不要なライセンス情報を当該メモリから消去するようにしてもよい。

【０４３６】

なお、図１０７、図１１８に示した情報再生装置７０００は、汎用的なコンピュータに標準装備されているハードウエア資源を用いて構成することも可能である。

【０４３７】

また、本実施形態で説明したライセンス情報の復号鍵生成処理動作は、第２の実施形態で説明した復号ユニットＡ、Ｃの鍵生成部２００６においても適用できる。

【０４３８】

さらに、ライセンス情報に本実施形態で説明したようなライセンス認証情報が含まれている場合、ライセンス情報整合性確認部７００８ｃでライセンス認証情報を用いてライセンス情報が正しく復号されたか否かを確認する処理動作は、第２の実施形態で説明した復号ユニットＡ～Ｄの判定部２００３においても同様に行える。すなわち、復号ユニットＡ～Ｄの判定部２００３では、ライセンス認証情報を照合することにより、当該ライセンス情報が正しく復号できたと判断された後に所定のライセンス判定を行えばよい。

【０４３９】

以上説明したように、上記第４の実施形態によれば、ライセンス情報を復号するための鍵情報をライセンス判定ユニット７００８内で予め定められた時間毎に生成することにより、コンテンツ情報の利用条件やコンテンツ情報の復号化鍵を含むライセンス情報の情報セキュリティの向上が図れる。

【０４４０】

また、復号されたライセンス情報には、復号結果の正否を判定するためのライセンス認証情報が含まれていることにより、時間の経過に従って該ライセンス情報の復号化鍵がいくつも生成される状況であっても、そのうちのいずれか正しい復号鍵で当該ライセンス情報が復号されたか否かを容易に判断できる。

【０４４１】

また、ライセンス情報の復号化鍵は、情報再生装置に放送配信されてくるシード情報に基づきライセンス判定ユニット８００９内で生成されるので、当該復号鍵の更新が容易に行える。

（第５の実施形態）

（５－１）概略

図１２２は、第５の実施形態に係る情報流通システムの構成例を示したもので、課金対象である暗号化されたコンテンツ情報は、ＤＶＤ等のリムーバブル情報蓄積メディア（以下、簡単にディスクと呼ぶ）Ｄに予め記録されており、ディスクＤに記録されているコンテンツ情報を再生可能にするライセンスを購入してディスクＤを貸し出すことによりなるレンタルサービスを提供するためのものである。ここで、ライセンスとは、予め定められた条件下におけるレンタルされるディスクＤに記憶されているコンテンツ情報の利用（再生および視聴）権をいう。具体的には、例えば、限られた期間内、限られた回数だけ、コンテンツ情報を再生可能にするライセンス情報をユーザに売ることで、当該ライセンスを与えることになる。

【０４４２】

コンテンツ情報の再生を可能にするためのライセンス情報は、ＩＣカード等の演算機能を有するカード型記録媒体（以下、簡単にカードと呼ぶ）Ｐに記録して各ユーザに渡される。

【０４４３】

レンタル用のディスクＤを提供する各店舗には、ライセンス注入装置５００３が設置され、これらライセンス注入装置５００３とセンターとが所定の通信回線を介して接続されてネットワークを形成している。図１２２に示したような情報流通システムのサービスに加入しているユーザが、このネットワーク上の任意の店舗に赴き、所望のコンテンツ情報の記録されたディスクＤをレンタルするときは、まず、当該コンテンツ情報の視聴期間等のコンテンツ利用条件に対する料金の支払い等の所定の手続きを行う。ライセンス注入装置５００３は、センターから送られてきた当該ディスクＤのディスクキーと利用条件等を含むディスク情報に基づきライセンス情報を作成して、カードＰに記録する。

【０４４４】
ユーザは、ディスクＤおよびカードＰを持ち帰り、カードＰを当該情報流通システムに適合したカードアダプタ５００４に挿入し、ディスクＤをプレーヤー５００５にセットすることにより、ライセンス情報に含まれる利用条件を満たす限り（例えば視聴期間内であれば）、当該コンテンツ情報の再生が可能となる。
【０４４５】
図１２３は、店舗にあるレンタル用のディスクＤに記録されているデータの一例を示したものである。図１２３に示すように、ディスクＤには、ディスクＩＤ、１または複数の（例えば２種類の）暗号化コンテンツ情報、コンテンツ情報を復号するための各コンテンツ情報のそれぞれに対応する暗号化されたコンテンツキーとが記録されている。
【０４４６】
１枚のディスクに記録されているコンテンツ情報は、そのそれぞれに対応するコンテンツキーにて暗号化されており、そのコンテンツキーは、当該ディスクのディスクＩＤに予め定められたディスクキーにて暗号化されている。ディスクキーは当該ディスクには記録されていないことが特徴である。
【０４４７】
ディスクＩＤは各ディスクを識別するための識別情報で、各ディスク毎にユニークに定められていても良いし、同一タイトルのコンテンツ情報を記憶するディスクに共通であっても良い。あるいは、同じ製造工場で同じ日に製造されたディスクのディスクＩＤは共通であってもよい。
【０４４８】
ディスクＩＤに対して、そのディスクに記録されている暗号化コンテンツキーを復号することのできるディスクキー（ディスク内には含まれていないが）は一意に定まる。が、逆は必ずしも真ではない。即ち、コンテンツキーを復号する為のディスクキーが同じであるからと言って、ディスクＩＤが同じであるとは限らない。
【０４４９】
レンタル用のディスクＤには、図１２３に示したようにディスクキーが含まれていない。ディスクＤをレンタルするときは、そのディスクＤに記憶されているコンテンツを復号するために必要なディスクキーをユーザに配信する必要がある。
【０４５０】
そこで、ディスクＤをレンタルする際には、センタに設けられたライセンス作成装置５００１で当該ディスクＤに対応するディスクキーを含むディスク情報を作成するようになっている。ディスクキーは、例えば図１２４に示したように、センタに設けられたコンテンツＤＢ５００２にディスクＩＤに対応させて予め記憶されている。
【０４５１】
本発明は、ディスクキーの安全な配送方式を提供するものである。
【０４５２】
図１２５に、図１２２に示した情報流通システムにおけるディスクキーの配送方式を概略的に示したものである。大きく分けて、ライセンス作成装置５００１とライセンス注入装置５００３とで鍵（ディスクキー）配信装置を構成し、カードアダプタ５００４とプレーヤ５００５とで鍵配信装置から配信された鍵（ディスクキー）を用いてコンテンツ情報を利用（例えば再生）する情報利用装置を構成する。ライセンスの有効性を判定するための判定装置はカードアダプタ３００４が具備している。
【０４５３】
ディスクキーが、ライセンス作成装置５００１からカードアダプタ５００４に送りとどけられるまで、ディスクＩＤ、コンテンツの利用条件とともに暗号化鍵ｋｅで暗号化されている。すなわち、ライセンス情報作成装置５００１では、ディスクキーとディスクＩＤと利用条件とを含むディスク情報を作成し、さらに暗号化鍵ｋｅで暗号化してから配信し、復号化鍵ｋｄを予め保持しているカードアダプタ５００４で復号することにより、途中の配信経路で盗聴等されてもディスクキーが解読される危険性を低くすることができる。

【０４５４】
なお、鍵配信装置を構成するライセンス作成装置５００１とライセンス注入装置５００３とは、互いに利害関係を有する異なる者に別個に属する場合があり、その場合には、その利害関係を調整するために（ライセンス作成装置５００１からライセンス注入装置５００３へ配信する過程でディスク情報を不正に取得されることがないようにするため）、ライセンス作成装置５００１では、ディスク情報を暗号化してからライセンス注入装置５００３へ配信することが望ましい。
【０４５５】
ディスクキーを含む暗号化されたディスク情報がカードアダプタ５００４に到達するまでには、ライセンス注入装置５００３、カードＰとを経由する。そこで、この間における配信経路上でディスク情報を保護するため、暗号化されたディスク情報をさらに暗号化してライセンス注入装置５００３からカードアダプタ５００４まで配信する。
【０４５６】
例えば、図１２５に示すように、ライセンス注入装置５００３では、ライセンス作成装置５００１から配信された暗号化鍵ｋｄで暗号化されたディスク情報に他の情報データを付加してライセンス情報を作成し、そのライセンス情報を共通鍵ｗｌ２で暗号化してカードＰに書き込む。
【０４５７】
共有鍵ｗｌ２は、例えば、ＤＨ鍵配送方式（Ｄｉｆｆｉｅ－ｈｅｌｌｍａｎ　Ｋｅｙ　Ｄｉｓｔｒｉｂｕｔｉｏｎ　Ｓｃｈｅｍｅ）のように、カードＰを介してカードアダプタ５００４とライセンス注入装置５００３との間で交換される公開してもかまわない情報（公開パラメータ）と、カードアダプタ５００４とライセンス注入装置５００３のそれぞれで保持される秘密パラメータとから生成される。公開パラメータはカードアダプタ５００４とライセンス注入装置５００３のそれぞれで保持される秘密パラメータから生成される。公開パラメータだけを知っている盗聴者は共有鍵ｗｌ２は作れないようになっている。
【０４５８】
共有鍵ｗｌ２で暗号化されたディスク情報を復号できるのは、公開パラメータをライセンス注入装置５００３と交換し合ったカードアダプタ５００４だけである。
【０４５９】
カードアダプタ５００４は、カードＰを介してライセンス注入装置５００３から配信された公開パラメータと、自身で保持する秘密パラメータとから共有鍵ｗｌ２を生成し、この共有鍵を用いて、同じくカードＰを介してライセンス注入装置５００３から配信された暗号化ライセンス情報を復号し、暗号化ディスク情報を得る。この暗号化ディスク情報を、復号化鍵ｋｅを用いて復号し、利用条件等をチェックして再生可否を判定する。再生可と判定したときは、ディスク情報に含まれるディスクキーをプレーヤ５００５に渡す。
【０４６０】
カードアダプタ５００４とプレーヤ５００５との間が盗聴されるかもしれない安全でない通信路であるならば、やはり、ディスクキーを暗号化してから配信することが望ましい。そこで、例えば、ＤＨ鍵配送方式のように、カードアダプタ５００４とプレーヤ５００５との間で交換される公開パラメータと、カードアダプタ５００４とプレーヤ５００４のそれぞれで保持される秘密パラメータとから生成される共有鍵ｗｄ２を用いて、カードアダプタ５００４でディスクキーを暗号化してからプレーヤ５００５へ配信する。
【０４６１】
ライセンス作成装置５００１でディスクキーを暗号化する際、ディスクＩＤ、コンテンツの利用条件等を付加してディスク情報を作成してから暗号化する。また、ライセンス注入装置５００３でディスク情報を暗号化する際には、カードＰの識別情報（ＫＩＤ）、カードアダプタ５００４の識別情報（ＡＩＤ）等を付加してライセンス情報を付加してから暗号化する。ライセンス情報には、さらに、当該ライセンス情報の作成時刻が含まれていてもよい。
【０４６２】

カードアダプタ５００４およびカードＰでは、それぞれの識別情報が外部から読取り、修正等が不可能なように保護されていることが望ましい。

【０４６３】

ライセンス情報にカードＰの識別情報（ＫＩＤ）、カードアダプタ５００４の識別情報（ＡＩＤ）を含める場合、ライセンス注入装置５００３は、ライセンス情報を作成する以前に、ＫＩＤ、ＡＩＤを取得する必要がある。

【０４６４】

カードＰから、その識別情報ＫＩＤをライセンス注入装置５００３へ配信するときは、ＫＩＤを暗号化してから配信することが望ましい。そこで、例えば、ＤＨ鍵配送方式のように、ライセンス注入装置５００３とカードＰとの間で交換される公開パラメータと、ライセンス注入装置５００３とカードＰとのそれぞれで保持される秘密パラメータとから生成される共有鍵ｗｋを用いて、カードＰで識別情報ＫＩＤを暗号化してからライセンス注入装置５００３へ配信する。

【０４６５】

カードアダプタ５００４から、その識別情報ＡＩＤをライセンス注入装置５００３へ（カードＰを介して）配信するときは、ＡＩＤを暗号化してから配信することが望ましい。そこで、例えば、ＤＨ鍵配送方式のように、ライセンス注入装置５００３とカードアダプタ５００４との間で交換される公開パラメータと、ライセンス注入装置５００３とカードアダプタ５００４とのそれぞれで保持される秘密パラメータとから生成される共有鍵ｗｌ１を用いて、カードアダプタ５００４で識別情報ＡＩＤを暗号化してからライセンス注入装置５００３へ配信する。

ライセンス情報にカードＰの識別情報（ＫＩＤ）、カードアダプタ５００４の識別情報（ＡＩＤ）が含まれているとき、カードアダプタ５００４では、ライセンス情報に基づき再生可否を判定する際、カードアダプタ５００４自身のＡＩＤと、現在カードアダプタ５００４に挿入されているカードＰのＫＩＤと照合することができ、より情報セキュリティの向上が図れる。

【０４６６】

図１２５に示すように、ディスクキーをライセンス作成装置５００１からユーザ側の情報再生装置へ安全に配信するために、その配信経路上の各機器には、以下に示すような秘密パラメータを含む秘密情報を保持している。

【０４６７】

・ライセンス作成装置５００１は、ディスク情報を暗号化するための暗号化鍵Ｋｅを保持し、カードアダプタ５００４はディスク情報を復号するための復号化鍵Ｋｄを保持している。

【０４６８】

・カードアダプタ５００４とライセンス注入装置５００３とは、両者が互いに認証し合い、ライセンス情報の暗号化復号化のために用いる、数Ｘ（ｌ）と、同一のシードを与えた時同一の鍵を生成する鍵生成アルゴリズムＡｌ（Ｐｌ）と、十分大なる素数Ｐｒｌとを共有する。これらは、両者の認証と、ライセンス情報の暗号化復号化のために用いられる。ただし、ＰｌはアルゴリズムＡｌのパラメータで、カードアダプタ５００４とライセンス注入装置５００３とは、アルゴリズムＡｌ及びパラメータＰｌとを共有している。Ｘ（ｌ）、Ａｌ、Ｐｌ、Ｐｒｌは、カードアダプタ５００４とライセンス注入装置５００３とに外部からの読み取りが困難である様に保護されて記憶されている。

【０４６９】

・ライセンス注入装置５００３とカードＰとは、数Ｘ（ｋ）と、同一のシードを与えた時同一の鍵を生成する鍵生成アルゴリズムＡｋ（Ｐｋ）と、十分大なる素数Ｐｒｋとを共有する。これらは、両者の認証と、カードＰの識別情報ＫＩＤの暗号化復号化のために用いられる。ただし、ＰｋはアルゴリズムＡｋのパラメータであり、ライセンス注入装置５００３とカードＰとは、アルゴリズムＡｋ及びパラメータＰｋとを共有している。Ｘ（ｋ）、Ａｋ、Ｐｋ、Ｐｒｋは、ライセンス注入装置５００３とカードＰとに外部からの読み取

りが困難なように保護されて記憶されている。
【０４７０】
・カードアダプタ５００４とカードＰとは、数Ｘ（ｋ）と、同一のシードを与えた時同一の鍵を生成する鍵生成アルゴリズムＡｋ（Ｐｋ）と、十分大なる素数Ｐｒｋを共有する。これらは、両者の認証と、カードＰの識別情報ＫＩＤの暗号化復号化のために用いられる。ただし、ＰｋはアルゴリズムＡｋのパラメータであり、カードアダプタ５００４とカードＰとは、アルゴリズムＡｋ及びパラメータＰｋとを共有している。Ｘ（ｋ）、Ａｋ、Ｐｋ、Ｐｒｋは、ライセンス注入装置５００３とカードＰとに外部からの読み取りが困難である様に保護されて記憶されている。
【０４７１】
・カードアダプタ５００４とプレーヤー５００５とは、数Ｘ（Ｄ）と、同一のシードを与えた時同一の鍵を生成する鍵生成アルゴリズムＡＤ（ＰＤ）と、充分大なる素数ＰｒＤを共有する。これは、両者の認証と、ディスクキーの暗号化復号化のために用いられる。ただし、ＰＤはアルゴリズムＡＤのパラメータであり、カードアダプタ５００４とプレーヤー５００５とはアルゴリズムＡＤとパラメータＰＤとを共有している。Ｘ（Ｄ）、ＡＤ、ＰＤ、ＰｒＤは、カードアダプタ５００４とプレーヤー５００５とに外部からの読み取りが困難である様に保護されて記憶されている。
【０４７２】
・プレーヤー５００５は復号化鍵ＫｐＤ、カードＰは復号化鍵ＫｐＣ、カードアダプタ５００４は復号化鍵ＫｐＡ、ライセンス注入装置５００３は復号化鍵ＫｐＬをそれぞれ外部からの読み取りが困難である様に保護されて記憶されている。復号化鍵ＫｐＤ、ＫｐＣ、ＫｐＡ、ＫｐＬは、公開鍵暗号方式の公開鍵である。これらに対応する４つの秘密鍵ＫｓＤ、ＫｓＡ、ＫｓＣ、ＫｓＬは、ライセンス作成装置５００１が保持している。これら公開鍵および秘密鍵は、前述のＸ（ｌ）、Ｘ（ｋ）、Ｘ（Ｄ）、パラメータＰｌ、Ｐｋ、ＰＤ、素数Ｐｒｌ、Ｐｒｋ、ＰｒＤ等を更新する際に利用される。
【０４７３】
このように、ディスクキーは、暗号技術によって２重に保護されて配信されている。
【０４７４】
（５－２）ライセンス作成装置
図１２６は、ライセンス作成装置５００１の構成例を示したもので、以下、図１３１に示すフローチャートを参照しながら、ライセンス作成装置５００１の構成およびディスク情報作成処理動作について説明する。
【０４７５】
ディスク情報の作成は、例えば１２時間毎に行われる。簡単の為、コンテンツの利用条件として、視聴可能期限（有効期限）を用い、コンテンツの視聴可能期間は１週間と予め定められたライセンスを与えるディスク情報を作成するものとする。
【０４７６】
さて、視聴可能期間の開始時刻は０時及び１２時であるとしよう。ライセンス作成装置５００１は、例えば３時間前にディスク情報の作成を開始する。即ち、２１時と９時にディスク情報の作成を開始する。視聴可能期間が９時から開始されるライセンスを与えるディスク情報の作成について述べる。９時に時計５００１ａから情報取得部５００１ｂに対してディスク情報作成指示が発行される（ステップＳ５００１～ステップＳ５００２）。情報取得部５００１ｂは有効期限作成部５００１ｃに対して時計５００１ａから受け取った現在の日時情報（例えば、１９８１年４月２日９時）を送信する（ステップＳ５００３）。
【０４７７】
有効期限作成部５００１ｃは、日時情報に基づき、その日の１２時から起算して一週間後の有効期限の日時（例えば、１９８１年４月９日１２時）を情報取得部５００１ｂに返す（ステップＳ５００４）。次いで、情報取得部５００１ｂは、コンテンツＤＢ５００２から、ディスクＩＤとディスクキーの１対の情報を読み出し、それを有効期限とマージして

ディスク情報を作成し、第１の暗号化部５００１ｄへ転送する（ステップＳ５００５）。ディスク情報には、ディスクＩＤ、ディスクキー、有効期限とが含まれている。

【０４７８】

第１の暗号化部５００１ｄは、第１の暗号鍵格納部５００１ｅから暗号化鍵ｋｅを読み出し、ディスク情報を暗号化する（ステップＳ５００６）。当該暗号化ディスク情報は平文のディスクＩＤが付加されて、所定のネットワークを経由してライセンス注入装置５００３へ配信される（ステップＳ５００７）。

【０４７９】

以上ステップＳ５００５～ステップＳ５００７の処理を繰り返し、コンテンツＤＢ５００２に登録されている全てのコンテンツＩＤについてのディスク情報を作成する（ステップＳ５００８）。

【０４８０】

ライセンス注入装置５００３は、ライセンス作成装置５００１から受信した暗号化ディスク情報を、内部のライセンスＤＢ５００３ｆ（図１２７参照）に、図１３２に示すように、ディスクＩＤに対応させて記憶する。

【０４８１】

ディスク情報に有効期限が含まれていることは重要である。ライセンス注入装置５００３は店舗に置かれ、攻撃の対象になりにくいとは言え、万一の盗難と言うことも考えられる。しかし、有効期限が含まれているディスク情報は、永久のライセンスを保証しないので、ライセンス注入装置５００３を盗む動機は弱められる。のみならず、ディスク情報を解読して永久ライセンスの窃盗（即ち、ディスクキーの取得）を試みる為には、カードアダプタ５００４に格納されている復号鍵Ｋｄ及びディスク情報の暗号化復号化用の秘密情報を盗む必要がある。ところが、復号鍵Ｋｄも秘密情報もハードウェア的に厳重に保護されていれば、この作業は非常に困難である。

【０４８２】

（５－３）ライセンス注入装置

図１２７はライセンス注入装置５００３の構成例を示したものである。

【０４８３】

カードＰは、カード装着部５００３ａに挿入される。カード装着確認部５００３ｂにより、カードＰが正常に装着されていることが確認されると、カードＰとライセンス注入装置５００３とは、カード装着部５００３ａを介して通信可能な状態となる。

【０４８４】

乱数生成部５００３ｋは、カードＰのＩＤ（ＫＩＤ）、カードアダプタ５００４のＩＤ（ＡＩＤ）、ライセンス情報（Ｌｉｃ）の暗号化・復号化に用いる乱数ａｌ、ｃｌ、ａｋを発生する。

【０４８５】

ベース格納部５００３ｍには秘密パラメータＸ（ｌ）、Ｐｒｌ、Ｘ（ｋ）、Ｐｒｋとが予め格納されている。

【０４８６】

巾乗演算部５００３ｊは、乱数生成部５００３ｋで発生された乱数とベース格納部５００３ｍに格納されている秘密パラメータとから公開パラメータ（第１～第３のシード生成情報）を計算する。また、カードＰから転送されてくる第１のシード生成情報と乱数生成部５００３ｋで発生された乱数ａｋとから第１のシードを生成する。また、カードＰを介してカードアダプタ５００４から転送されてくる第２のシード生成情報と乱数生成部５００３ｋで発生された乱数ａｌとから第２のシードを生成する。また、カードＰを介してカードアダプタ５００４から転送されてくる第２のシード生成情報と乱数生成部５００３ｋで発生された乱数ｃｌとから第３のシードを生成する。

【０４８７】

例えば、乱数ａｌと秘密パラメータ（Ｘ（ｌ）、Ｐｒｌ）とから第２のシード生成情報$X(l)^{al}$（ｍｏｄ　Ｐｒｌ）を計算する。以下、巾乗を表す場合、記号「＾」を用いて、

「Ｘ（ｌ）＾ａｌ」と記す。また、ｍｏｄは剰余（この場合、Ｘ（ｌ）^{al}を素数Ｐｒｌで乗算したときの剰余）を表す。また、乱数ａｋと秘密パラメータ（Ｘ（ｋ）、Ｐｒｋ）とから第１のシード生成情報Ｘ（ｋ）＾ａｋ（ｍｏｄ　Ｐｒｋ）を計算する。

【０４８８】

共有鍵生成部５００３ｌには、鍵生成アルゴリズムＡｌ（Ｐｌ）、Ａｋ（Ｐｋ）が予め格納されている。第１のシードにアルゴリズムＡｋ（Ｐｋ）を適用して第１の共有鍵ｗｋ１を生成し、第２のシードにアルゴリズムＡｌ（Ｐｌ）を適用して第２の共有鍵ｗｌ１を生成し、第３のシードにアルゴリズムＡｌ（Ｐｌ）を適用して第３の共有鍵ｗｌ２を生成する。第１～第３のシードに鍵生成アルゴリズムＡｌ（Ｐｌ）、Ａｋ（Ｐｋ）を適用することにより、第１～第３のシードのデータ長を小さくすることができる。

【０４８９】

復号部５００３ｄは、共有鍵生成部５００３ｌで生成された共有鍵ｗｋ１、ｗｌ１、を用いて、暗号化されたカードＩＤ（［ＫＩＤ］ｗｋ１）、暗号化されたカードアダプタＩＤ（［ＡＩＤ］ｗｌ１）を復号する。

【０４９０】

ディスク接続部５００３ｇには、ユーザがレンタル使用とするディスクＤが挿入されて、当該ディスクＤのＩＤ（ＤＩＤ）を読み取る。

【０４９１】

カードデータベース（ＤＢ）５００３ｉは、ユーザに発行されるカードＰのＩＤとそれに対応するカードアダプタ５００４のＩＤとの対応関係を記憶するためのものである。

【０４９２】

ライセンスデータベース（ＤＢ）５００３ｆは、ライセンス作成装置５００１から転送されてきた暗号化ディスク情報を記憶するためのもので、図１３２に示すように、暗号化ディスク情報は、ディスクＩＤ（ＤＩＤ）との対応させて記憶されている。

【０４９３】

ライセンス作成部５００３ｅは、ユーザがディスクをレンタルしようとする際に、そのディスクに対するライセンスを作成する。すなわち、ディスク接続部５００３ｇで読み取られた当該ディスクＤのＩＤ（ＤＩＤ）をキーとしてライセンスＤＢ５００３ｆから暗号化ディスク情報を検索し、カードＤＢ５００３ｉからユーザの所持するカードＰと、カードアダプタ５００４のＩＤ（ＫＩＤ、ＡＩＤ）を読み取り、さらに、時計５００３ｈから現在時刻を読み取って、暗号化ディスク情報、ライセンス作成時刻、ＫＩＤ、ＡＩＤを含むライセンス情報を作成する。

【０４９４】

なお、ここで作成されたライセンス情報は、カードＰを介してカードアダプタ５００４との間で交換された公開パラメータに基づき生成される共有鍵ｗｌ２で暗号化される。

【０４９５】

制御部５００３ｃは、ライセンス注入装置５００３全体の制御を司るものである。

【０４９６】

（５－４）カード

図１２８は、カードＰの構成例を示したものである。

【０４９７】

カードＰは、機器装着部５１０１を介して、ライセンス注入装置５００３、カードアダプタ５００４に接続し、機器装着確認部５１０２により、カードＰがライセンス注入装置５００３あるいはカードアダプタ５００４に正常に装着されていることが確認されると、カードＰとライセンス注入装置５００３あるいはカードアダプタ５００４とは、機器装着部５１０１を介して通信可能な状態となる。

乱数生成部５１０７は、カードＰのＩＤ（ＫＩＤ）をライセンス注入装置５００３およびカードアダプタ５００４へ転送する際に、カードＩＤ（ＫＩＤ）の暗号化・復号化に用いる乱数ｂｋ、ｄｋを発生する。

【０４９８】

ベース格納部５１０９には、秘密パラメータＸ（ｋ）、ＰｒｋとＡが予め格納されている。
【０４９９】
巾乗演算部５１０６は、乱数生成部５１０７で発生された乱数とベース格納部５１０９に格納されている秘密パラメータとから公開パラメータ（第１のシード生成情報、第５のシード生成情報）を計算する。また、ライセンス注入装置５００３から転送されてくる第１のシード生成情報と乱数生成部５１０７で発生された乱数ｂｋとから第１のシードを生成する。またカードアダプタ５００４から転送されてくる第５のシード生成情報と乱数生成部５１０７で発生された乱数ｄｋとから第５のシードを生成する。
【０５００】
共有鍵生成部５１０８には、鍵生成アルゴリズムＡｋ（Ｐｋ）が予め格納されている。第１のシードにアルゴリズムＡｋ（Ｐｋ）を適用して第１の共有鍵ｗｋ１を生成し、第５のシードにアルゴリズムＡｋ（Ｐｋ）を適用して第５の共有鍵ｗｌ１を生成する。第１、第５のシードに鍵生成アルゴリズムＡｋ（Ｐｋ）を適用することにより、第１、第５のシードのデータ長を小さくすることができる。
ＫＩＤ格納部５１０５には、当該カードＰを一意に識別するためのＩＤ（識別情報）、すなわち、ＫＩＤが予め格納されている。
【０５０１】
ＫＩＤ暗号化部５１０４は、ＫＩＤ格納部５１０５に格納されているＫＩＤを共有鍵生成部５１０８で生成された共有鍵ｗｋ１、ｗｋ２で暗号化する。
【０５０２】
制御部５１０３は、カードＰ全体の制御を司るものである。
【０５０３】
（５－５）カードアダプタ
カードＰは、カード装着部５００４ａに挿入される。カード装着確認部５００４ｂにより、カードＰが正常に装着されていることが確認されると、カードＰとカードアダプタ５００４とは、カード装着部５００４ａを介して通信可能な状態となる。
【０５０４】
乱数生成部５００４ｋは、ＡＩＤ格納部５００４ｆに予め格納されている自身のＩＤ（ＡＩＤ）、ライセンス情報（Ｌｉｃ）、プレーヤにセットされたディスクＤのＩＤ（ＤＩＤ）、カードＰのＩＤ（ＫＩＤ）、ディスクキーの暗号化・復号化に用いる乱数ｂｌ、ａＤ、ｃｋ、ｄＤを発生する。
【０５０５】
乱数格納部５００４ｌは、乱数生成部５００４ｋで発生された乱数ｂｌ、ａＤ、ｃｋを記憶する。
【０５０６】
ベース格納部５００４ｍには秘密パラメータＸ（ｌ）、Ｐｒｌ、Ｘ（ｋ）、Ｐｒｋ、Ｘ（Ｄ）、ＰｒＤとが予め格納されている。
【０５０７】
巾乗演算部５００４ｊは、乱数生成部５００４ｋで発生された乱数とベース格納部５００４ｍに格納されている秘密パラメータとから公開パラメータ（第２、第４、第５、第６のシード生成情報）を計算する。また、カードＰを介してライセンス注入装置５００３から転送されてくる第２のシード生成情報と乱数生成部５００４ｋで発生された乱数ｂｌとから第２のシードを生成する。また、カードＰを介してライセンス注入装置５００３から転送されてくる第３のシード生成情報と乱数生成部５００４ｋで発生された乱数ｂｌとから第３のシードを生成する。また、プレーヤ５００５から転送されてくる第４のシード生成情報と乱数生成部５００４ｋで発生された乱数ａＤとから第４のシードを生成する。また、カードＰから転送されてくる第５のシード生成情報と乱数生成部５００３ｋで発生された乱数ｃｋとから第５のシードを生成する。プレーヤ５００５から転送されてくる第６のシード生成情報と乱数生成部５００４ｋで発生された乱数ｄＤとから第６のシードを生成する。

【０５０８】
共有鍵生成部５００４ｉには、鍵生成アルゴリズムＡｌ（Ｐｌ）、Ａｋ（Ｐｋ）、ＡＤ（ＰＤ）が予め格納されている。第２のシードにアルゴリズムＡｌ（Ｐｌ）を適用して第２の共有鍵ｗｌ１を生成し、第３のシードにアルゴリズムＡｌ（Ｐｌ）を適用して第３の共有鍵ｗｌ２を生成し、第４のシードにアルゴリズムＡＤ（ＰＤ）を適用して第４の共有鍵ｗＤ１を生成し、第５のシードにアルゴリズムＡｋ（Ｐｋ）を適用して第５の共有鍵ｗｋ２を生成し、第６のシードにアルゴリズムＡＤ（ＰＤ）を適用して第６の共有鍵ｗＤ２を生成する。第２～第６のシードに鍵生成アルゴリズムＡｌ（Ｐｌ）、Ａｋ（Ｐｋ）を適用することにより、第２～第６のシードのデータ長を小さくすることができる。
【０５０９】
暗号化／復号化部５００４ｏは、共有鍵生成部５００４ｉで生成された共有鍵ｗＤ２でディスクキーを暗号化する。また、共有鍵生成部５００４ｉで生成された共有鍵ｗｌ２、ｗＤ１、ｗｋ２を用いて暗号化ライセンス情報［Ｌｉｃ］ｗｌ２、暗号化ディスクＩＤ［ＤＩＤ］ｗＤ１、暗号化カードＩＤ［ＫＩＤ］ｗｋ２を復号する。
【０５１０】
ＡＩＤ格納部５００４ｆには、当該カードアダプタ５００４を一意に識別するためのＩＤ（識別情報）、すなわち、ＡＩＤが予め格納されている。
【０５１１】
ＡＩＤ暗号化部５００４ｄは、ＡＩＤ格納部５００４ｆに格納されているＡＩＤを共有鍵生成部５００４ｉで生成された共有鍵ｗｌ１で暗号化する。
【０５１２】
ｋｄ格納部５００４ｇには、暗号化鍵ｋｅで暗号化されたディスク情報を復号するための復号化鍵ｋｄが格納されている。
【０５１３】
プレーヤ接続部５００４ｍには、プレーヤ５００５がカードアダプタ５００４と通信可能なように接続されている。
【０５１４】
ライセンス判定部５００４ｅは、カードＰを介してライセンス注入装置５００３から転送されてきたライセンス情報に含まれる暗号化ディスク情報を復号か鍵ｋｄで復号する。ライセンス判定処理（図１３９～図１４０）では、以下の条件をチェックする。
・ライセンス情報に含まれるカードＩＤ（ＫＩＤ）およびカードアダプタＩＤ（ＡＩＤ）と、ライセンス判定部５００４ｅに挿入されたカードＰのカードＩＤ（ＫＩＤ）およびＡＩＤ格納部５００４ｆに格納されているカードアダプタＩＤ（ＡＩＤ）とが一致していること
・ライセンス情報の作成時刻が時計５００４ｈの現在表示時刻より以前であること
・ディスク情報に含まれるディスクＩＤ（ＤＩＤ）とプレーヤ５００５に現在セットされているディスクＤのＩＤとが一致していること
・時計５００４ｈの現在表示時刻がディスク情報に含まれる有効期限を満たすこと
以上の条件を満たすとき、ライセンス判定部５００４ｅは、ディスク情報に含まれるディスクキーをプレーヤ５００５へ出力する。その際、ディスクキーは、プレーヤ接続部５００４ｎを介してプレーヤ５００５との間で交換される第６のシード生成情報に基づき生成される共有鍵ｗＤ２で暗号化されている。
【０５１５】
（５－６）プレーヤ
カードアダプタ接続部５００５ａには、カードアダプタ５００４がプレーヤ５００５と通信可能なように接続されている。
【０５１６】
乱数生成部５００５ｉは、ディスクドライブ５００５ｄにセットされているディスクＤから読み取ったディスクＤのＩＤ（ＤＩＤ）、ディスクキーの暗号化・復号化に用いる乱数ｂＤ、ｃＤを発生する。

【０５１７】
乱数格納部５００５ｋは、乱数生成部５００５ｉで発生された乱数ｃＤを記憶する。
【０５１８】
ベース格納部５００５ｌには秘密パラメータＸ（Ｄ）、ＰｒＤが予め格納されている。
【０５１９】
巾乗演算部５００５ｈは、乱数生成部５００５ｉで発生された乱数とベース格納部５００５ｌに格納されている秘密パラメータとから公開パラメータ（第４、第６のシード生成情報）を計算する。また、カードアダプタ５００４から転送されてくる第４のシード生成情報と乱数生成部５００５ｉで発生された乱ｂＤとから第４のシードを生成する。また、カードアダプタ５００４から転送されてくる第６のシード生成情報と乱数生成部５００５ｉで発生された乱ｃＤとから第６のシードを生成する。
【０５２０】
共有鍵生成部５００５ｊには、鍵生成アルゴリズムＡＤ（ＰＤ）が予め格納されている。第４のシードにアルゴリズムＡＤ（ＰＤ）を適用して共有鍵ｗＤ１を生成する。第６のシードにアルゴリズムＡＤ（ＰＤ）を適用して共有鍵ｗＤ２を生成する。第４、第６のシードに鍵生成アルゴリズムＡＤ（ＰＤ）を適用することにより、第４、第６のシードのデータ長を小さくすることができる。
【０５２１】
ディスクドライバ５００５ｄには、ディスクＤがセットされて、ディスクＤに記憶されているディスクＩＤ（ＤＩＤ）、暗号化コンテンツ情報、暗号化コンテンツキーが読み出される。ディスクＩＤ（ＤＩＤ）は、ＤＩＤ暗号化部５００５ｃへ転送され、暗号化コンテンツ情報および暗号化コンテンツキーは再生部５００５ｆへ転送される。
【０５２２】
ＤＩＤ暗号化部５００５ｃは、ディスクＩＤ（ＤＩＤ）を共有鍵生成部５００５ｊで生成された共有鍵ｗＤ１暗号化する。
【０５２３】
ディスクキー復号部５００５ｅは、暗号化ディスクキー［ディスクキー］ｗＤ２を共有鍵生成部５００５ｊで生成された共有鍵ｗＤ２で復号する。復号されたディスクキーは再生部５００５ｆへ転送される。
【０５２４】
再生部５００５ｆは、暗号化コンテンツキーをディスクキーを用いて復号し、復号されたコンテンツキーを用いて暗号化コンテンツ情報を復号し、再生して、出力部５００５ｇへ出力する。
【０５２５】
（５－７）ディスクキーの配信手順（その１）
次に、図１３３に示すシーケンス図および図１３４～図１４０に示すフローチャートを参照して、図１２２の情報流通システムにおけるディスクキーの配信手順の概略をディスクレンタルサービスへの加入時、ディスクのレンタル時、コンテンツ再生時の順に説明する。
【０５２６】
まず、ディスクレンタルサービスへの加入時について説明する。
【０５２７】
ステップｘ１：　ユーザに発行されるカードＰは、ライセンス注入装置５００３に挿入する。ライセンス注入装置５００３は、乱数ａｌを発生する。カードアダプタ５００４のＩＤ（ＡＩＤ）を取得するため、乱数ａｌと秘密パラメータ（Ｘ（ｌ）、Ｐｒｌ）とから、ＡＩＤを暗号化するために必要な公開パラメータ、すなわち、第２のシード生成情報Ｘ（ｌ）＾ａｌ（ｍｏｄ　Ｐｒｌ）を計算し、カードＰに転送する。（図１３４のステップＳ６００１～ステップＳ６００３）。
【０５２８】
ステップｘ２：　さらに、ライセンス注入装置５００３は、乱数ａｋを発生する。カード

ＰのＩＤ（ＫＩＤ）を取得するために、乱数ａｋと秘密パラメータ（Ｘ（ｋ）、Ｐｒｋ）とから第１のシード生成情報Ｘ（ｋ）＾ａｋ（ｍｏｄ　Ｐｒｋ）を計算し、カードＰに転送する（図１３５のステップＳ６０１０～ステップＳ６０１１）。

【０５２９】

ステップｘ３：　カードＰは、第１のシード生成情報を受け取り、乱数ｂｋを発生する。乱数ｂｋと第１のシード生成情報とから第１のシード（Ｘ（ｋ）＾ａｋ）＾ｂｋ＝Ｘ（ｋ）＾（ａｋ・ｂｋ）（ｍｏｄ　Ｐｒｋ）を計算する。この第１のシードに、予め格納されているアルゴリズムＡｋ（Ｐｋ）を適用して共有鍵ｗｋ１を生成する。共有鍵ｗｋ１を用いてカードＰのＩＤ（ＫＩＤ）を暗号化する。以下、共有鍵ｗｋ１で暗号化されたＫＩＤを［ＫＩＤ］ｗｋ１と記す。さらに、乱数ｂｋと秘密パラメータ（Ｘ（ｋ）、Ｐｒｋ）とから［ＫＩＤ］ｗｋ１を復号するために必要な第１のシード生成情報Ｘ（ｋ）＾ｂｋ（ｍｏｄ　Ｐｒｋ）を計算し、［ＫＩＤ］ｗｋ１と、この第１のシード生成情報とをライセンス注入装置５００３へ転送する（図１３５のステップＳ６０１２～ステップＳ６０１６）。

【０５３０】

ライセンス注入装置５００３では、カードＰから転送されてきた第１のシード生成情報と、先に発生した乱数ａｋとから第１のシードを生成する。この第１のシードに、予め格納されているアルゴリズムＡｋ（Ｐｋ）を適用して共有鍵ｗｋ１を生成し、［ＫＩＤ］ｗｋ１を復号して、カードＰのＩＤ（ＫＩＤ）を得る（ステップＳ６０１７～ステップＳ６０１９）。

【０５３１】

このようにして取得されたカードＰのＩＤは、カードデータベース（ＤＢ）５００３ｉに、先に発生した乱数ａｌに対応させて記憶される（図１３５のステップＳ６０２１）。カードＤＢ５００３ｉに記憶された情報は、後に、カードＰを介して取得されるカードアダプタのＩＤ（ＡＩＤ）を復号する際に用いられる。この時点で、カードＰには、ライセンス注入装置から受け取った第２のシード生成情報Ｘ（ｌ）＾ａｌ（ｍｏｄ　Ｐｒｌ）が格納されている。

【０５３２】

ステップｘ４：　ユーザは、以上の処理を施されたカードＰを持ち帰り、自宅にあるカードアダプタ５００４に当該カードＰを挿入する。すると、カードアダプタ５００４では、カードＰから第２のシード生成情報を読み取る。また、カードアダプタ５００４は、乱数ｂｌを発生し、この乱数ｂｌと第２のシード生成情報とから第２のシードＸ（ｌ）＾（ａｌ・ｂｌ）（ｍｏｄ　Ｐｒｌ）を計算する。この第２のシードに予め格納されているアルゴリズムＡｌ（Ｐｌ）を適用して共有鍵ｗｌ１を生成する。そして、共有鍵ｗｌ１を用いて当該カードアダプタ５００４の識別情報ＡＩＤを暗号化する。以下、共有鍵ｗｌ１で暗号化されたＡＩＤを［ＡＩＤ］ｗｌ１と記す。

【０５３３】

ステップｘ５：　先に発生した乱数ｂｌと秘密パラメータ（Ｘ（ｌ）、Ｐｒｌ）とから第２のシード生成情報Ｘ（ｌ）＾ｂｌ（ｍｏｄ　Ｐｒｌ）を計算し、この第２のシード生成情報と［ＡＩＤ］ｗｌ１とをカードＰに転送する（図１３４のステップＳ６００４～ステップＳ６００９）。

【０５３４】

この時点で、カードＰには、第２のシード生成情報と［ＡＩＤ］ｗｌ１とが記憶されていることになる。このとき、カードＰでは、先に格納していた第２のシード生成情報Ｘ（ｌ）＾ａｌ（ｍｏｄ　Ｐｒｌ）を消去しても良い。カードアダプタ５００４は、後にライセンス情報を復号する為に、乱数ｂｌを乱数格納部５００４ｌに記憶しておく。

【０５３５】

ユーザがディスクをレンタルしようとするときは、カードＰを持参して、例えばディスクレンタルサービスの加盟店舗（ライセンス注入装置５００３が設置されている店舗）に行き、所望のディスクを選択して、カードＰとともに店員に差し出す。

【０５３６】
ステップｘ６～ステップＳｘ７：　差し出されたカードＰとディスクＤはライセンス注入装置５００３に挿入される。ライセンス注入装置５００３は、当該カードＰのＩＤ（ＫＩＤ）を取得するために、前述のステップｘ２～ステップｘ３と同様にして、カードＰから当該カードＰの識別情報を得る（図１３４のステップＳ６００１、図１３５のステップＳ６０１０～ステップＳ６０１９）。なお、このとき発生される乱数ａｋ、ｂｋは、前述のステップｘ２～ステップｘ３における乱数ａｋ、ｂｋと必ずしも一致しないが、この事はＫＩＤの取得に何ら影響を与えない。
【０５３７】
ステップｘ８：　カードＰはラインセンス注入装置５００３へ第２のシード生成情報と［ＡＩＤ］ｗｌ１を転送する。ライセンス注入装置５００３は、カードＤＢ５００３ｉから、ステップｘ７で取得したカードＩＤ（ＫＩＤ）に対応する乱数ａｌを検索する。前述した適正なる手続き処理を経たカードＰであるならば、そのカードＩＤ（ＫＩＤ）に対応する乱数ａｌがカードＤＢ５００３ｉに登録されているはずである。ライセンス注入装置５００３は、カードＰから転送された第２のシード生成情報と検索された乱数ａｌとから第２のシードＸ（ｌ）＾（ａｌ・ｂｌ）（ｍｏｄ　Ｐｒｌ）を計算し、アルゴリズムＡｌ（Ｐｌ）を適用する事によって、共有鍵ｗｌ１を生成する。共有鍵ｗｌ１を用いて［ＡＩＤ］ｗｌ１を復号し、カードアダプタ５００４のＩＤ（ＡＩＤ）を得る（図１３５のステップＳ６０２０～ステップＳ６０２１、図１３６のステップＳ６０２２～ステップＳ６０２６）。
【０５３８】
ライセンス注入装置５００３は、カードＤＢ５００３ｉに、このカードアダプタ５００４の識別情報ＡＩＤをカードＰの識別情報に対応させて記憶する（図１３６のステップＳ６０２７）。
【０５３９】
かくして、ライセンス注入装置５００３は、ユーザに与えられたカードＩＤ（ＫＩＤ）とカードアダプタＩＤ（ＡＩＤ）との組み合わせを把握する事ができる。ユーザが複数のカードアダプタを使用している様な場合でも、上記ステップｘ１～ステップｘ８の手続きにより、ライセンス注入装置５００３は、ユーザの有する全てのカードアダプタのＩＤを把握する事ができる。その場合、カードＤＢ５００３ｉには、１つのカードＩＤ（ＫＩＤ）に対して複数のカードアダプタのＩＤ（ＡＩＤ）が対応付けられて記憶されることになる。
【０５４０】
ステップｘ９：　一方、ライセンス注入装置５００３は、挿入されたディスクＤから当該ディスクのＩＤ（ＤＩＤ）を取得して、ライセンスＤＢ５００３ｆから当該ディスクＩＤに対応する暗号化ディスク情報を取得する。この暗号化ディスク情報に、時計５００３ｈから取得した現在時刻をライセンス情報作成時刻としてマージし、カードＤＢ５００３ｉに含まれる情報（ユーザのカードＩＤ（ＫＩＤ）やカードアダプタＩＤ（ＡＩＤ））を必要に応じてマージしてライセンス情報（Ｌｉｃ）を作成する。すなわち、
Ｌｉｃ＝暗号化ディスク情報＋ライセンス情報作成時刻（＋ＡＩＤ＋ＫＩＤ）
である。ＡＩＤ、ＫＩＤをライセンス情報Ｌｉｃに含めるか否かは、例えば、店舗の判断による。或いは、ライセンス作成装置５００１がＡＩＤ、ＫＩＤの要不要を決定し、その決定内容をライセンスＤＢ５００３ｆにカードＩＤに対応させて（付加情報として）記録して置いても良い（この場合、ライセンス注入装置５００３は、この付加情報があれば、それに従ってＡＩＤ、ＫＩＤをライセンス情報Ｌｉｃにマージするばよい）。ライセンス情報ＬｉｃにＡＩＤを含めるという事は、ライセンスを特定のカードアダプタに限定する事を意味する。又、ライセンス情報ＬｉｃにＫＩＤを含めるという事は、ライセンスを特定のカードに限定する事を意味する（図１３６のステップＳ６０２８～ステップＳ６０３０）。
【０５４１】

さて、ライセンス注入装置５００３は、乱数ｃｌを発生する。カードＰから既に第２のシード生成情報Ｘ（ｌ）＾ｂｌ（ｍｏｄ　Ｐｒｌ）を読み取っているから、ライセンス注入装置５００３は、乱数ｃｌとこの第２のシード生成情報とから第３のシードＸ（ｌ）＾（ｂｌ・ｃｌ）（ｍｏｄ　Ｐｒｌ）を計算する。この第３のシードにアルゴリズムＡｌ（Ｐｌ）を適用して、鍵ｗｌ２を生成して、ライセンス情報Ｌｉｃを暗号化する。以下、共有鍵ｗｌ２で暗号化されたライセンス情報Ｌｉｃを［Ｌｉｃ］ｗｌ２と記す。さらに、乱数ｃｌと秘密パラメータ（Ｘ（ｌ）、ｐｒｌ）とから［ｌｉｃ］ｗｌ２を復号するために必要な公開パラメータ、すなわち、第３のシード生成情報Ｘ（ｌ）＾ｃｌ（ｍｏｄ　Ｐｒｌ）を計算し、この第３のシード生成情報と暗号化ライセンス情報［Ｌｉｃ］ｗｌ２とをカードＰに転送する（図１３６のステップＳ６０３１～ステップＳ６０３５）。

この時点で、カードＰには、暗号化ライセンス情報［Ｌｉｃ］ｗｌ２と第３のシード生成情報とが記憶されていることになる。先にカードＰに記憶されていた［ＡＩＤ］ｗｌ１は、既にライセンス注入装置５００３に渡されたので、消去されてもよい。

【０５４２】

ユーザは、以上の処理を施されたカードＰとディスクＤとを持ち帰り、自宅にあるカードアダプタ５００４、プレーヤ５００５を用いてコンテンツの再生を行うことができる。

【０５４３】

ステップｘ１１：　コンテンツを再生するために、ユーザがカードＰをカードアダプタ５００４へ挿入し、ディスクＤをプレーヤ５００５にセットする。カードアダプタ５００４は、カードＰから暗号化ライセンス情報［Ｌｉｃ］ｗｌ２と第３のシード生成情報とを読み出し、この第３のシード生成情報とステップｘ５で一時格納された乱数ｂｌとから第３のシードＸ（ｌ）＾（ｂｌ・ｃｌ）（ｍｏｄ　Ｐｒｌ）を計算する。この第３のシードにアルゴリズムＡｌ（Ｐｌ）を適用して、共有鍵ｗｌ２を生成し、暗号化ライセンス情報［Ｌｉｃ］ｗｌ２を復号する（図１３８のステップＳ６０４６～ステップＳ６０４９）。

【０５４４】

ステップｘ１２：　一方、プレーヤ５００５は、セットされたディスクＤからディスクＩＤ（ＤＩＤ）を読取る。

【０５４５】

ステップｘ１３：　カードアダプタ５００４は、乱数ａＤを発生する。カードアダプタ５００４は、プレーヤ５００５からこのディスクＤのディスクＩＤ（ＤＩＤ）を取得するため、プレーヤ５００５へディスクＩＤ（ＤＩＤ）を暗号化するために必要な公開パラメータ、すなわち、第４のシード生成情報を生成する。すなわち、乱数ａＤと、秘密パラメータ（Ｘ（Ｄ）、ＰｒＤ）とから第４のシード生成情報Ｘ（Ｄ）＾ａＤ（ｍｏｄ　ＰｒＤ）計算し、これをプレーヤ５００５へ転送する（図１３７のステップＳ６０３６～ステップＳ６０３７）。

【０５４６】

ステップｘ１４：　プレーヤ５００５は、この第４のシード生成情報を受け取ると、乱数ｂＤを発生し、第４のシード生成情報とこの乱数ｂＤとから第４のシードＸ（Ｄ）＾（ａＤ・ｂＤ）（ｍｏｄ　ＰｒＤ）を計算し、アルゴリズムＡＤ（ＰＤ）を適用して、共有鍵ｗＤ１を生成し、ディスクＩＤ（ＤＩＤ）を暗号化する。以下、共有鍵ｗＤ１で暗号化されたＤＩＤを［ＤＩＤ］ｗＤ１と記す。さらに、乱数ｂＤと秘密パラメータ（Ｘ（Ｄ）、ＰｒＤ）とから［ＤＩＤ］ｗＤ１を復号するために必要な公開パラメータ、すなわち、第４のシード生成情報Ｘ（Ｄ）＾ｂＤ（ｍｏｄ　ＰｒＤ）を計算し、［ＤＩＤ］ｗＤ１と、この第４のシード生成情報とをカードアダプタ５００４へ転送する（図１３７のステップＳ６０３８～ステップＳ６０４２）。

【０５４７】

カードアダプタ５００４では、プレーヤ５００５から転送されてきた第４のシード生成情報と［ＤＩＤ］ｗＤ１とを受け取ると、第４のシード生成情報と、乱数ａＤとから第４のシードＸ（Ｄ）＾（ａＤ・ｂＤ）（ｍｏｄ　ＰｒＤ）を計算する。この第４のシードにアルゴリズムＡＤ（ＰＤ）を適用して共有鍵ｗＤ１を生成し、［ＤＩＤ］ｗＤを復号してデ

ィスクＩＤ（ＤＩＤ）を取得する（図１３７のステップＳ６０４３～ステップＳ６０４５）。

【０５４８】

次に、図１３８のステップＳ６０５０に進み、ライセンス情報に基づくコンテンツ情報の復号可否を判定する処理（ライセンス判定処理）を行う（図１３９～図１４０）。

【０５４９】

ライセンス情報にカードアダプタのＩＤが含まれている場合、カードアダプタ５００４は、ＡＩＤ格納部５００４ｆに格納されているカードアダプタＩＤ（ＡＩＤ）とライセンス情報に含まれているカードアダプタＩＤ（ＡＩＤ）とを比較する。これが一致しなければ、当該ライセンス情報は、当該カードアダプタ５００４に適合するものではないので、処理を停止する。ＡＩＤが一致すれば、次の処理に進む（図１３９のステップＳ６０６１～ステップＳ６０６２）。

【０５５０】

ステップｘ１５：　ライセンス情報にカードＩＤが含まれている場合、カードアダプタ５００４は、カードＰからその識別情報ＫＩＤを取得するため、まず、乱数ｃｋを発生し、カードＰのカードＩＤ（ＫＩＤ）を暗号化するために必要な公開パラメータ、すなわち、第５のシード生成情報を生成する。すなわち、乱数ｃｋと秘密パラメータ（Ｘ（ｋ）、Ｐｒｋ）とから第５のシード生成情報Ｘ（ｋ）＾ｃｋ（ｍｏｄ　Ｐｒｋ）を計算し、カードＰに転送する（図１３９のステップＳ６０６３～ステップＳ６０６５）。

【０５５１】

ステップｘ１６：　カードＰは、第５のシード生成情報を受け取ると、乱数ｄｋを発生し、この第５のシード生成情報と乱数ｄｋとから第５のシードＸ（ｋ）＾（ｃｋ・ｄｋ）（ｍｏｄ　Ｐｒｋ）を計算する。第５のシードにアルゴリズムＡｋ（Ｐｋ）を適用して、鍵ｗｋ２を生成し、カードＰのカードＩＤ（ＫＩＤ）を暗号化する。以下、共有鍵ｗｋ２で暗号化されたＫＩＤを［ＫＩＤ］ｗｋ２と記す。さらに、乱数ｄｋから［ＫＩＤ］ｗｋ２を復号するために必要な公開パラメータ、すなわち、第５のシード生成情報Ｘ（ｋ）＾ｄｋ（ｍｏｄ　Ｐｒｋ）を計算し、この第５のシード生成情報と［ＫＩＤ］ｗｋ２とをカードアダプタ５００４へ転送する（ステップＳ６０６６～ステップＳ６０７０）。

【０５５２】

カードアダプタ５００４では、カードＰから転送されてきた第５のシード生成情報と乱数ｃｋとから第５のシードを計算する。この第５のシードにアルゴリズムＡｋ（Ｐｋ）を適用して、鍵ｗｋ２を生成し、［ＫＩＤ］ｗｋ２からＫＩＤを復号する。このカードＰから送られてきたカードＩＤ（ＫＩＤ）と、ライセンス情報に含まれていたカードＩＤ（ＫＩＤ）とが一致する場合、次の処理に進む。さもなければ、カードＰに記憶されていたライセンス情報が当該カードＰに不適合であったわけであるから、以後の処理を停止する（ステップＳ６０７１～ステップＳ６０７４）。

【０５５３】

ステップｘ１７：　次に、カードアダプタ５００４は、ライセンス情報に含まれるライセンス情報作成時刻をチェックする。ライセンス情報作成時刻をＴｌと表す事にする。カードアダプタ５００４は時計５００４ｈから現在表示時刻Ｔｃを取得する。Ｔｃ＜＝Ｔｌのときは現在表示時刻Ｔｃが遅れている事を示している。実際、ライセンス情報が作成された時刻Ｔｌは、現在表示時刻Ｔｃよりも前でなければならない筈である。従って、Ｔｃ＜＝Ｔｌのときは、カードアダプタ５００４は、時計５００４ｈが不正確であると判断し、以後の処理を停止する。或いは、若干の許容誤差範囲Ｔｅ（＞０）を予め設定しておき、Ｔｃ＞Ｔｌ＋Ｔｅが成立する時及びその時に限って、以後の処理に進む様にしても良い（図１４０のステップＳ６０７５）。

【０５５４】

次に、予め保持されていた復号化鍵ｋｄを用いてライセンス情報に含まれていた暗号化ディスク情報を復号する（ステップＳ６０７６）。ディスク情報には、ディスクＩＤ（ＤＩＤ）、ディスクキー、有効期限（ＴＬ）とが含まれている。まず、有効期限ＴＬと時計６

００４ｈの現在表示時刻Ｔｃとを比較する。ＴＬ＜Ｔｃであれば、ライセンスは有効期限は切れているので、カードアダプタ５００４は以後の処理を停止する。或いは、若干の許容誤差Ｔｅ′（＞０）を予め設定しておき、Ｔｃ≦ＴＬ＋Ｔｅ′が成立する時及びその時に限って、以後の処理に進む様にしても良い（ステップＳ６０７７）。

【０５５５】

最後に、カードアダプタ５００４は、ディスク情報に含まれるディスクＩＤ（ＤＩＤ）と、先に取得したディスクＤのディスクＩＤとを比較して、両者が一致しなければ、当該ライセンス情報は、現在プレーヤ５００５にセットされているディスクＤとは異なるディスクに対するものであるから、以後の処理を中止する。ディスクＩＤが一致した場合に、当該ディスクＤに記録されているコンテンツ情報の再生が可能と判定される（ステップＳ６０７８）。

【０５５６】

再生可と判定されたとき、カードアダプタ５００４は、ディスク情報に含まれていたディスクキーをプレーヤ５００５へ転送するため、まず、プレーヤ５００５に対して、乱数の発生を指示する。

【０５５７】

ステップｘ１８：　乱数発生の指示を受けたプレーヤー５００５は、乱数ｃＤを発生し、この乱数ｃＤと秘密パラメータ（Ｘ（Ｄ）、ＰｒＤ）とから第６のシード生成情報Ｘ（Ｄ）＾ｃＤ（ｍｏｄ　ＰｒＤ）を計算し、カードアダプタ５００４に転送する（図１３８のステップＳ６０５１～ステップＳ６０５２）。

【０５５８】

ステップｘ１９：　カードアダプタ５００４は、第６のシード生成情報を受け取ると、乱数ｄＤを発生する。第６のシード生成情報と乱数ｄＤとから第６のシードＸ（Ｄ）＾（ｃＤ・ｄＤ）（ｍｏｄ　ＰｒＤ）を計算し、この第６のシードにアルゴリズムＡＤ（ＰＤ）を適用して、ディスクキー暗号化用の共有鍵ｗＤ２を生成し、ディスクキーを共有鍵ｗＤ２で暗号化する。以下、共有鍵ｗＤ２で暗号化されたディスクキーを［ディスクキー］ｗＤ２と記す。さらに、乱数ｄＤと秘密パラメータ（Ｘ（Ｄ）、ＰｒＤ）とから［ディスクキー］ｗＤ２を復号するために必要な公開パラメータ、すなわち、第６のシード生成情報Ｘ（Ｄ）＾ｄＤ（ｍｏｄ　ＰｒＤ）を計算し、この第６のシード生成情報と［ディスクキー］ｗＤ２とをプレーヤ５００５へ転送する（ステップＳ６０５３～ステップＳ６０５６）。

【０５５９】

プレーヤ５００５では、カードアダプタ５００４から転送されてきた第６のシード生成情報と乱数ＣＤとから第６のシードＸ（Ｄ）＾（ｃＤ・ｄＤ）（ｍｏｄＰｒＤ）を計算する。この第６のシードに、アルゴリズムＡＤ（ＰＤ）を適用して、共有鍵ｗＤ２を生成し、［ディスクキー］ｗＤ２を復号する（ステップＳ６０５７～ステップＳ６０５９）。

【０５６０】

プレーヤ５００５は、このディスクキーを用いて、ディスクＤに記憶されている暗号化コンテンツキーを復号し、さらに、このコンテンツキーで暗号化コンテンツ情報の復号・再生を行うことができる（ステップＳ６０６０）。

【０５６１】

なお、暗号化ディスク情報の復号化鍵Ｋｄをプレーヤ５００５に格納する事も可能である。この場合、暗号化ディスク情報を復号するのはプレーヤ５００５である。ライセンス情報作成時刻、有効期限等の有効性を判定するために参照される時計５００４ｈはカードアダプタ５００４であるので、有効期限を暗号化ディスク情報に含めることができない。従って、この様な場合、ライセンス作成装置５００１からライセンス注入装置５００３に転送される暗号化ディスク情報の構成要素は、「ディスクＩＤ＋ディスクキー」となる。有効期限は、ライセンス注入装置５００３が設定し、前述のステップｘ９でライセンス情報の作成する際に、暗号化ディスク情報に有効期限をマージして、暗号化ディスク情報、ライセンス情報作成時刻、有効期限、必要に応じてカードＩＤ（ＫＩＤ）とカードアダプタ

ＩＤ（ＡＩＤ）を含むライセンス情報を作成すればよい。
【０５６２】
カードアダプタ５００４では、復号化鍵Ｋｄによるディスク情報の復号を行うことなく有効期限の有効性を判定する。
【０５６３】
復号化鍵Ｋｄをプレーヤ５００５に保持させるメリットは、
・ライセンス注入装置５００３に蓄積される暗号化ディスク情報が有効期限を含んでいない為、ディスク情報を更新する必要がない。すなわち、ライセンス作成装置５００１は新たに追加されたレンタル用のディスクの暗号化ディスク情報だけを作成し、ライセンス注入装置５００３へ適宜転送すれば良い。
【０５６４】
一方、ディメリットは、
・暗号化ディスク情報が更新されることがないので、ライセンス注入装置５００３の不正使用に対する動機を強めてしまう。
【０５６５】
・プレーヤ５００５内の復号化鍵Ｋｄを保護する為に、プレーヤ５００５のセキュリティを高めなくてはならない。
【０５６６】
さて、以上のディスクキーの配信手順によれば、ユーザが行う手順を簡単に説明する。
【０５６７】
ｉ）ディスクレンタルサービスへの加入時に、ユーザは、当該ディスクレンタルサービスの加盟店舗でカードＰの発行を受ける。場合によっては、この際にカードアダプタ５００４を購入する、又はカードアダプタ５００４の貸与を受ける。
【０５６８】
ii）ユーザが自宅でプレーヤ５００５に接続されたカードアダプタ５００４にカードＰを挿入する。
【０５６９】
iii）ユーザがディスクをレンタルするときには、カードＰをもって、店舗に赴き、所望のレンタルディスクＤを選択し、代金と引き換えに、カードＰにライセンスの注入を受ける。
【０５７０】
iv）ユーザがディスクＤとカードＰとを自宅に持ち帰り、カードアダプタ５００４にカードＰを挿入して、ディスクＤを再生する。ライセンス有効期間中、ディスクＤを幾度でも再生する事ができる。
【０５７１】
ｖ）以後、ユーザがディスクをレンタルする際には、上記iii）～iv）を繰り返す。
【０５７２】
（５－８）ディスクキーの配信手順（その２）
ところで、ディスクレンタルサービスへの加入時に、カードＰの発行を受けると同時に、ディスクがレンタルできれば、一層ユーザにとって便利である。この場合のユーザが行う手順を簡単に説明する。
【０５７３】
ｉ）ディスクレンタルサービスへの加入時に、ユーザは、当該ディスクレンタルサービスの加盟店舗でカードＰの発行を受ける。場合によっては、この際にカードアダプタ５００４を購入する、又はカードアダプタ５００４の貸与を受ける。
【０５７４】
ii’） ユーザは、所望のレンタルディスクＤを選択し、代金と引き換えに、カードＰにライセンスの注入を受ける。
【０５７５】
iii’）ユーザは、ディスクＤとカードＰとを自宅に持ち帰り、カードアダプタ５００４

にカードＰを挿入して、ディスクＤを再生する。ライセンス有効期間中、ディスクを幾度でも再生する事ができる。

【０５７６】

ｉｖ’）以後、ユーザがディスクをレンタルする際には、上記ｉｉ’）～ｉｉｉ’）を繰り返す。

【０５７７】

次に、このような場合のディスクキーの配信手順について説明する。

【０５７８】

図１４１に示すシーケンス図および図１４２～図１４６に示すフローチャートを参照して、図１２２の情報流通システムにおけるディスクキーの他の配信手順の概略をディスクレンタルサービスへの加入・ディスクのレンタル時、コンテンツ再生時の順に説明する。

【０５７９】

ディスクレンタルサービスに加入しているユーザに提供される全てのカードアダプタ５００４およびライセンス注入装置５００３は、乱数ｂｌ０を共有している。乱数ｂｌ０は、例えばＲＯＭ等に記憶されていて、カードアダプタ外部から読み出すのは困難なように保護されていることが望ましい。

【０５８０】

乱数ｂｌ０は、ライセンス注入装置５００３、カードアダプタ５００４のそれぞれのベース格納部５００３ｍ、５００４ｍに予め格納されているものとする。

まず、ディスクレンタルサービスへの加入時について説明する。

【０５８１】

ステップｙ１～ステップｙ２：　ユーザに発行されるカードＰは、ライセンス注入装置５００３に挿入する。ライセンス注入装置５００３は、図１３３のステップｘ２～ステップｘ３、ステップｘ６～ステップｘ７と同様にして、カードＰからカードＩＤ（ＫＩＤ）を取得する（図１４２のステップＳ６１０１～ステップＳ６１１０）。

【０５８２】

ステップｙ３：ユーザにより選択されたレンタルディスクＤもライセンス注入装置５００３に挿入される。ライセンス注入装置５００３は、挿入されたディスクＤから当該ディスクのＩＤ（ＤＩＤ）を取得して、ライセンスＤＢ５００３ｆから当該ディスクＩＤに対応する暗号化ディスク情報を取得する。

【０５８３】

ライセンス注入装置５００３は、時計５００３ｈから取得した現在時刻をライセンス情報作成時刻としてマージし、さらに、ユーザのカードＩＤ（ＫＩＤ）をマージしてライセンス情報（Ｌｉｃ）を作成する（図１４２のステップＳ６１１１～ステップＳ６１１４）。

すなわち、

Ｌｉｃ＝暗号化ディスク情報＋ライセンス情報作成時刻＋ＫＩＤ

である。

【０５８４】

ステップｙ４：　次に、ライセンス注入装置５００３は、乱数ａｌを発生する。そして、カードＤＢ５００３ｉにカードＰのカードＩＤと乱数ａｌとを記憶する。

【０５８５】

乱数ａｌと例えば、秘密パラメータ（Ｘ（ｌ）、ｐｒｌ）とから第７のシードＸ（ｌ）＾（ａｌ・ｂｌ０）（ｍｏｄ　Ｐｒｌ）を計算し、さらに、この第７のシードにアルゴリズムＡｌ（Ｐｌ）を適用して、共有鍵ｗｌ３を生成し、ライセンス情報Ｌｉｃを暗号化する。以下、共有鍵ｗｌ３で暗号化されたライセンス情報Ｌｉｃを［Ｌｉｃ］ｗｌ３と記す。さらに、乱数ａｌと秘密パラメータ（Ｘ（ｌ）、ｐｒｌ）とから［ｌｉｃ］ｗｌ３を復号するために必要な公開パラメータ、すなわち、第７のシード生成情報Ｘ（ｌ）＾ａｌ（ｍｏｄ　Ｐｒｌ）を計算し、この第７のシード生成情報と暗号化ライセンス情報［Ｌｉｃ］ｗｌ３とをカードＰに転送する（図１４２のステップ６１１５～ステップｘ６１１９）。

【０５８６】

この時点で、カードＰには、暗号化ライセンス情報［Ｌｉｃ］ｗｌ３と第７のシード生成情報とが記憶されていることになる。

【０５８７】

ユーザは、以上の処理を施されたカードＰとディスクＤとを持ち帰り、自宅にあるカードアダプタ５００４、プレーヤ５００５を用いてコンテンツの再生を行うことができる。

【０５８８】

ステップｙ５：　コンテンツを再生するために、ユーザがカードＰをカードアダプタ５００４へ挿入し、ディスクＤをプレーヤ５００５にセットする。カードアダプタ５００４は、カードＰから暗号化ライセンス情報［Ｌｉｃ］ｗｌ３と第７のシード生成情報とを読み出し、この第７のシード生成情報とベース格納不５００４ｍに予め格納された乱数ｂｌ０とから第７のシードＸ（ｌ）＾（ａｌ・ｂｌ０）（ｍｏｄ　Ｐｒｌ）を計算する。この第７のシードにアルゴリズムＡｌ（Ｐｌ）を適用して、共有鍵ｗｌ３を生成し、暗号化ライセンス情報［Ｌｉｃ］ｗｌ３を復号する。カードアダプタ５００４は、さらに、ライセンス情報に含まれていた暗号化ディスク情報を復号化鍵Ｋｄで復号する（図１４３のステップＳ６１２０～ステップＳ６１２９）。

【０５８９】

ステップｙ８～ステップｙ９：　カードアダプタ５００４は、図１３３のステップｘ１５～ステップｘ１６と同様にしてカードＰからカードＩＤ（ＫＩＤ）を取得する（図１４３のステップＳ６１３０～ステップＳ６１３９）。

【０５９０】

ステップｙ１０～ステップｙ１２：　カードアダプタ５００４は、さらに、図１３３のステップｘ１２～ステップｘ１４と同様にしてディスクＤのディスクＩＤ（ＤＩＤ）を取得する（図１４４のステップＳ６１４０～ステップＳ６１４９）。

【０５９１】

ステップｙ１３：　次に、図１４５のステップＳ６１５０に進み、ライセンス情報に基づくコンテンツ情報の復号可否を判定する処理（ライセンス判定処理）を行う（図１４６）。

【０５９２】

ライセンス判定処理（図１４６）では、以下の条件をチェックする。

・ライセンス情報に含まれるカードＩＤ（ＫＩＤ）と、カードアダプタ５００４に挿入されたカードＰのカードＩＤとが一致していること

・ディスク情報に含まれるディスクＩＤ（ＤＩＤ）とプレーヤ５００５に現在セットされているディスクＤのディスクＩＤとが一致していること

・ライセンス情報の作成時刻が時計５００４ｈの現在表示時刻より以前であること

・時計５００４ｈの現在表示時刻がディスク情報に含まれる有効期限を満たすこと

以上の条件を満たすときのみ、カードアダプタ５００４は、当該ディスクＤに記録されているコンテンツ情報の再生が可能であると判定し、ディスク情報に含まれていたディスクキーをプレーヤ５００５へ転送するため、まず、プレーヤ５００５に対して、乱数の発生を指示する。

【０５９３】

ステップｙ１４～ステップｙ１５：　図１３３のステップｘ１８～ステップｘ１９と同様にして、ディスクキーは、プレーヤ５００５との間で交換される第６のシード生成情報に基づき生成される共有鍵ｗＤ２で暗号化されて、プレーヤ５００５へ転送される（図１４５のステップＳ６１５０～ステップＳ６１６１）。

ステップｙ６～ステップｙ７：　一方、カードアダプタ５００４は、上記ライセンス判定処理に前後して、カードＰにＡＩＤ格納部５００４ｆに予め格納されているカードアダプタＩＤ（ＡＩＤ）を転送する処理を実行する。その際、カードアダプタＩＤ（ＡＩＤ）は、図１３３のステップｘ４～ステップｘ５と同様にして、カードＰを介してライセンス注入装置５００３から転送されてきた第７のシード生成情報（第２のシード生成情報と同じもの）と、乱数生成部５００４ｋで発生した乱数ｂｌとに基づき生成される共有鍵ｗｌ１

で暗号化される。
【０５９４】
２回目のディスクレンタル時以降は、図１３３のステップｘ６～ステップｘ１９と同様である。なお、２回目のディスクレンタル時に、ライセンス注入装置５００３は、図１３３のステップｘ８でユーザの所持するカードアダプタのＩＤ（ＡＩＤ）を取得することができる。すなわち、カードＤＢ５００３ｉにカードＰのカードＩＤ（ＫＩＤ）とカードアダプタＩＤ（ＡＩＤ）との対応関係が登録される。
【０５９５】
（５－９）暗号パラメータの更新
本発明のディスクキーを含むライセンス情報の配信は、配信経路上の各装置の持つ秘密パラメータと各装置間で交換される（秘密パラメータから生成される）公開パラメータとに基づき相手認証と転送保護とを行っている。従って、定期的に、或いはセキュリティに対する攻撃の疑いがある場合に適宜、秘密パラメータや暗号化ディスク情報の復号化鍵ｋｄ等（以下、これらをまとめて暗号パラメータと呼ぶ）を更新する事が望ましい。この更新は、ライセンス作成装置５００１が主導して行うことが望ましい。
【０５９６】
ライセンス作成装置５００１が更新する暗号パラメータは、例えば、（Ｘ（ｌ）、Ｐｌ、Ｐｒｌ）（Ｘ（ｋ）、Ｐｋ、Ｐｒｋ）（Ｘ（Ｄ）、ＰＤ、ＰｒＤ）（Ｋｄ、Ｋｅ）であるとして、図１４７～図１４９に示すフローチャートを参照して、暗号パラメータ更新処理について説明する。
【０５９７】
ライセンス作成装置５００１の暗号パラメータ生成部５００１ｈでは、上記暗号パラメータを例えば乱数発生器等を用いて更新する。次いで、各装置（プレーヤ５００５、カードアダプタ５００４、カードＰ、ライセンス注入装置５００３）用にパラメータ更新情報を作成する（図１４７のステップＳ６２０１）。
【０５９８】
プレーヤ用パラメータ更新情報は、Ｘ（Ｄ）、ＰＤ、ＰｒＤを含み、カードアダプタ用パラメータ更新情報はＸ（ｌ）、Ｐｌ、Ｐｒｌ、Ｘ（ｋ）、Ｐｋ、Ｐｒｋ、Ｘ（Ｄ）、ＰＤ、ＰｒＤ、Ｋｄを含み、カード用パラメータ更新情報はＸ（ｋ）、Ｐｋ、Ｐｒｋを含み、ライセンス注入装置用パラメータ更新情報はＸ（ｌ）、Ｐｌ、Ｐｒｌ、Ｘ（ｋ）、Ｐｋ、Ｐｒｋを含む。
【０５９９】
第２の暗号化部５００１ｇは、各装置用のパラメータ更新情報を、第２の暗号鍵格納部５００１ｆに予め格納されている暗号化鍵ＫｓＤ、ＫｓＡ、ＫｓＣ、ＫｓＬでそれぞれ暗号化する（ステップＳ６２０２～ステップＳ６２０３）。すなわち、プレーヤ用パラメータ更新情報は暗号鍵ＫｓＤで暗号化し、カードアダプタ用パラメータ更新情報は暗号鍵ＫｓＡで暗号化し、カード用パラメータ更新情報は暗号鍵ＫｓＰで暗号化し、ライセンス注入装置用パラメータ更新装置は暗号鍵ＫｓＬで暗号化する。以下、各装置用のそれぞれに対応した暗号化鍵で暗号化されたパラメータ更新情報を、例えば、プレーヤ用暗号パラメータの場合、［パラメータ更新情報］ＫｓＤと表す。
【０６００】
各装置用の暗号化パラメータ更新情報を以下に示す。
【０６０１】
プレーヤ用の暗号化パラメータ更新情報（ＵＤ）：［Ｘ（Ｄ）＋ＰＤ＋ＰｒＤ］ＫｓＤ
カードアダプタ用の暗号化パラメータ情報（ＵＡ）：［Ｘ（ｌ）＋Ｐｌ＋Ｐｒｌ＋Ｘ（ｋ）＋Ｐｋ＋Ｐｒｋ＋Ｘ（Ｄ）＋ＰＤ＋ＰｒＤ＋Ｋｄ］ＫｓＡ
カード用の暗号化パラメータ情報（ＵＣ）：［Ｘ（ｋ）＋Ｐｋ＋Ｐｒｋ］ＫｓＣ
ライセンス注入装置用の暗号化パラメータ情報（ＵＬ）：［Ｘ（ｌ）＋Ｐｌ＋Ｐｒｌ＋Ｘ（ｋ）＋Ｐｋ＋Ｐｒｋ］ＫｓＬ
時計５００１ａから現在表示時刻（暗号パラメータ更新時刻）を取得し、それを上記各装

置用の暗号化パラメータ情報とともに、ライセンス注入装置５００３へ転送する（ステップＳ６２０４～ステップＳ６２０５）。

【０６０２】

ライセンス注入装置は、各装置用の暗号化パラメータ情報（ＵＤ、ＵＡ、ＵＣ、ＵＬ）と更新時刻とを受信すると、暗号化パラメータ情報ＵＤ、ＵＡ、ＵＣ及び更新時刻を内部メモリに格納する（図１４８のステップＳ６２０６）。

【０６０３】

ライセンス注入装置５００４は、暗号化鍵ＫｓＬに対応する復号化鍵ＫｐＬを予めメモリに記憶しており、この復号化鍵ＫｐＬを用いて暗号化パラメータ更新情報ＵＬを復号し、ベース格納部５００３ｍ、共有鍵生成部５００３ｌに記憶されている暗号パラメータＸ（ｌ）、Ｐｌ、Ｐｒｌ、Ｘ（ｋ）、Ｐｋ、Ｐｒｋを更新する（ステップＳ６２０８）。なお、Ｐｌ及びＰｋは、夫々鍵生成アルゴリズムＡｌ、Ａｋのパラメータであったから、鍵生成アルゴリズムが更新される事になる。

【０６０４】

カードＰの暗号パラメータの更新処理動作は、カードＰがライセンス注入装置５００３に挿入された際、実行される。

【０６０５】

ユーザの所持するカードＰがライセンス注入装置５００３に挿入されると、ライセンス注入装置５００３は、カードＰから最新の暗号パラメータ更新時刻を取得する。この更新時刻が、ライセンス注入装置５００３に格納されている更新時刻（ライセンス作成装置５００１から転送されてきた更新時刻）より古いとき、ステップＳ６２１０へ進み、それ以外ときは、暗号パラメータ更新動作は終了し、ライセンス情報の書込み等、通常の処理動作を行う（ステップＳ６２０９）。

ステップＳ６２１０では、ライセンス注入装置５００３は、暗号化パラメータ更新情報ＵＤ、ＵＡ、ＵＣおよび更新時刻をカードＰに転送する。カードＰは、暗号化パラメータ更新情報ＵＤ、ＵＡ及び更新時刻を内部メモリに格納する。

【０６０６】

カードＰは、暗号化鍵ＫｓＣに対応する復号化鍵ＫｐＣを予めメモリに記憶しており、この復号化鍵ＫｓＣを用いて暗号化パラメータ更新情報ＵＣを復号し、ベース格納部５１０９、共有鍵生成部５１０８に記憶されている暗号パラメータＸ（ｋ）、Ｐｋ、Ｐｒｋを更新する（ステップＳ６２１１～ステップＳ６２１２）。その後、通常の処理動作を行う。

【０６０７】

カードアダプタ５００４の暗号パラメータの更新処理動作は、ユーザがカードＰをカードアダプタ５００４に挿入した際に実行される。すなわち、カードアダプタＩＤ（ＡＩＤ）をカードＰに転送する際、あるいは、ディスクＤを再生する為にカードＰからカードアダプタ５００４へライセンス情報を転送する際に、カードアダプタ５００４の暗号パラメータの更新処理が実行される。

【０６０８】

カードＰは、まず、カードＰの最新の暗号パラメータ更新時刻（ライセンス有入装置５００３から転送されてきた更新時刻）をカードアダプタ５００４へ転送する。カードアダプタ５００４は、この更新時刻がカードアダプタ５００４が記憶している最新の暗号パラメータの更新時刻より古いときはステップＳ６２１４へ進み、それ以外のときは、暗号パラメータ更新動作は終了し、通常の処理動作を行う（ステップＳ６２１３）。

【０６０９】

ステップＳ６２１４では、カードＰは、暗号化パラメータ更新情報ＵＤ、ＵＡ及び更新時刻、カードアダプタ５００４へ転送する。カードアダプタ５００４は、ＵＤ及び更新時刻を内部メモリに格納する。

【０６１０】

カードアダプタ５００４は、暗号化鍵ＫｓＡに対応する復号化鍵ＫｐＡを予めメモリに記憶しており、この復号化鍵ＫｐＡを用いて暗号化パラメータ更新情報ＵＡを復号し、ベー

ス格納部５１０９、共有鍵生成部５１０８、ｋｄ格納部５００４ｇに記憶されている暗号パラメータＸ（ｌ）、Ｐｌ、Ｐｒｌ、Ｘ（ｋ）、Ｐｋ、Ｐｒｋ、Ｘ（Ｄ）、ＰＤ、ＰｒＤ及びＫｄを更新する（ステップＳ６２１５～ステップＳ６２１６）。その後、通常の処理動作を行う。

【０６１１】

プレーヤ５００５の暗号パラメータの更新処理動作は、カードアダプタ５００４とプレーヤ５００５とが通信を行うとき実行される。すなわち、例えば、プレーヤ５００５からカードアダプタ５００４に対してディスクＩＤ（ＤＩＤ）を転送する際に、プレーヤ５００５の暗号パラメータの更新処理が実行される。

【０６１２】

例えば、プレーヤ５００５がカードアダプタ５００４にディスクＩＤ（ＤＩＤ）を転送する前に、まず、プレーヤ５００５の最新の暗号パラメータの更新時刻をカードアダプタ５００４へ転送する。

【０６１３】

カードアダプタ５００４は、プレーヤ５００５から転送されてきた更新時刻がカードアダプタ５００４が記憶している最新の暗号パラメータの更新時刻より古いときは、ステップＳ６２１８へ進み、それ以外のときは、暗号パラメータ更新動作は終了し、通常の処理動作を行う（ステップＳ６２１７）。

【０６１４】

ステップＳ６２１８では、カードアダプタ５０４は、暗号化パラメータ更新情報ＵＤ及び更新時刻をプレーヤ５００５へ転送する。プレーヤ５００５は、更新時刻を内部メモリに格納する。

【０６１５】

プレーヤ５００５は、暗号化鍵ＫｓＤに対応する復号化鍵ＫｐＤを予めメモリに記憶しており、この復号化鍵ＫｐＤを用いて暗号化パラメータ更新情報ＵＤを復号し、ベース格納部５００５ｌ、共有鍵生成部５００５ｊに記憶されている暗号パラメータＸ（Ｄ）、ＰＤ、ＰｒＤを更新する（ステップＳ６２１９～ステップＳ６２２０）。その後、通常の処理動作を行う。

【０６１６】

以上が、暗号パラメータの更新処理動作が終了する。暗号パラメータの更新は、ライセンス注入装置５００３に挿入される全てのカード（ユーザに発行された全てのカード）に対して行われる。従って、暗号パラメータの更新は、暗号パラメータの更新されたカードＰが挿入される全てのカードアダプタ５００４および該カードアダプタ５００４に接続されているプレーヤ５００５の全てに波及する。

【０６１７】

（５－１０）ディスクキーの配信手順（その３）

カードアダプタ５００４とプレーヤ５００５とが１つの装置として構成されている場合もあり得る（以下、第２のプレーヤと呼ぶ）。この場合のディスクキーを含めたライセンス情報の配信手順について、図１３３、図１４１を参照して簡単に説明する。すなわち、図１３３において、カードアダプタ５００４とプレーヤ５００５との間のディスクＩＤの転送処理（ステップｘ１３～ステップｘ１４）とディスクキーの転送処理（ステップｘ１８～ステップｘ１９）が不要となる。また、ステップｘ５において、カードＰを経由してライセンス注入装置５００３へ転送されるカードアダプタＩＤは、第２のプレーヤのＩＤ（ＰＩＤ）である。

【０６１８】

図１４１においてもカードアダプタ５００４とプレーヤ５００５との間のディスクＩＤの転送処理（ステップｙ１１～ステップｙ１２）とディスクキーの転送処理（ステップｙ１４～ステップｙ１５）が不要となる。また、ステップｙ７において、カードＰを経由してライセンス注入装置５００３へ転送されるカードアダプタＩＤは、第２のプレーヤのＩＤ（ＰＩＤ）である。

【０６１９】
それ以外は、前述同様である。
【０６２０】
以上説明したように、上記第５の実施形態によれば、コンテンツ情報を復号するために必要なディスクキーを、その配信元（ライセンス作成装置、ライセンス注入装置）から配信先（カードアダプタ、プレーヤ）までの安全に配信することができる。
（第６の実施形態）
図１５０は、本発明の第６の実施形態に係る情報流通システムの構成例を示したもので、課金対象である暗号化されたコンテンツ情報（著作物）は、ＤＶＤ等の情報記録メディア（以下、簡単にディスクと呼ぶ）７１０３に予め記録されており、ディスク７１０３に記録されているコンテンツ情報を再生可能にするライセンスを購入して、あるいは、当該コンテンツ情報の利用に対する点数（ポイント）を予め購入して、当該ディスク７１０３を貸し出すことによりなるレンタルサービスを提供するためのものである。すなわち、利用代金と引き換えにライセンス情報を提供する前述の実施形態で説明したようなライセンス方式とポイント方式とを組み合わせた超流通を実現することができる情報流通システムである。ポイント方式とは、プリペイドカード等に注入された著作物利用権をポイントとして利用者が予め購入しており、著作物の利用と引き換えに当該ポイントを減点する方式を言う。ポイント減点の際に著作物利用の明細（著作物のＩＤなど）をカードに記録し、カード回収の際に明細を回収し、プリペイドカード販売による収益の分配等に利用する方式を超流通と呼ぶ。
【０６２１】
ポイント方式は、ライセンス方式と比較して、次のメリットを有する。すなわち、予め店舗等で著作物の利用権であるポイントを購入しておけば、店舗にわざわざ出向くこと無く、著作物の利用ポイントと引き換えに、著作物を利用する事が可能である。
【０６２２】
ライセンス方式の場合でも、再生装置がライセンスサーバ（ライセンスの発行装置）と通信回線等を経由して接続可能であれば、店舗に出向くこと無く、著作物の利用権を入手する事は可能である。即ち、何らかのオンライン課金方式を利用して代金を支払い、ライセンス情報を入手すれば良い。ポイント方式のメリットは、オフライン（ライセンスサーバと接続されていない）状態で、著作物利用ポイントの減点による著作物利用権の取得が可能であるという点にある。
【０６２３】
一方、ポイント方式は、ライセンス方式と比較して、次のデメリットを有する。すなわち、著作物利用ポイントは、一種の著作物利用権購入用の金銭あるいは商品券であり、個別著作物のライセンスよりも、汎用的に使用可能である。従って、ライセンス方式よりも不正利用への動機付けが強い。ポイント方式のデメリットは、著作物利用ポイントの汎用性（例えば、利用権を購入した会員が利用する可能性のある再生装置以外の再生装置にも利用可能であるということ）に由来している。
【０６２４】
今、著作物レンタル業者により発行されたレンタル会員カード７１０２に、著作物利用ポイントを記録する場合を考える。当該著作物利用ポイントを含む機密性を有する情報（以下、ポイント情報と呼ぶ）の不正コピーなどを防止する観点から、会員カード７１０２に記録されるポイント情報は、会員が利用する再生装置が、そして当該再生装置のみが読み取り可能である事が望ましい。ところが、店舗で会員カードにポイント情報を記録する際に、会員が利用する可能性のある再生装置を特定する情報（再生装置のＩＤなど）を取得して、当該ポイント情報に組み込むことは、一般に不可能である。
【０６２５】
そこで、第６の実施形態では、ライセンス方式とポイント方式とを組み合わせて使用することによって、それぞれの方式のメリットを活かしつつ、デメリットを解消するものである。

【０６２６】
図１５０において、当該情報流通システムにより新規入会会員が、著作物情報（コンテンツ情報）が記録されたディスク７１０３を購入する（著作物利用権は購入代金に含まれていない）際には、ライセンス方式によって当該著作物のライセンス情報を取得する。即ち、ディスク７１０３とは別途当該著作物のライセンス情報を購入する。
【０６２７】
当該ディスク７１０３再生時に、会員の再生装置７１０１は会員カード７１０２からライセンス情報を読み取るが、その際、再生装置７１０１は、当該再生装置７１０１を一意的に特定でき、しかも、一度限り使用する情報（例えば、暗号鍵、乱数）Ｒをカードに記録する。
【０６２８】
会員は、次回の利用権購入からは、ライセンス情報の購入とともに、あるいはライセンス情報の購入に代えて、ポイント方式を利用する事が可能である。すなわち、２回目以降の利用権購入の際に、ポイント方式を利用する場合、店舗のライセンス／ポイント注入装置７１１１は、会員カード７１０２から情報Ｒを読み取り、情報Ｒを利用して、当該再生装置７１０１のみが利用できる形で、ポイント情報を会員カード７１０２に記録する。
【０６２９】
当該会員が再生装置７１０１にポイント情報が記録された会員カード７１０２を挿入すると、再生装置７１０１は会員カード７１０２からポイント情報を読み取り、その中に含まれるポイントを再生装置７１０１に格納する。ディスク７１０３を再生する際に、再生装置７１０１は当該格納したポイントから然るべき点数を減じる。
【０６３０】
なお、センター装置７１２１は、ライセンス／ポイント注入装置７１１１からの要求に応じて、ライセンス情報およびポイント情報を発行し、それを要求元のライセンス／ポイント注入装置７１１１に送信する。ライセンス／ポイント注入装置７１１１はセンター装置７１２１から送信されてきたライセンス情報、ポイント情報を会員カード７１０２に記録するようになっている。
【０６３１】
このようなシステムにより、
・　会員カードに記録されたポイントの利用が、特定の再生装置（当該会員の利用する可能性のある再生装置）に限定することができる
・　会員カードに記録されたポイント情報を最初に読み取った再生装置にのみ当該著作物の利用を限定することができる。
【０６３２】
従って、著作物利用に対し発行されるポイントの汎用性を限定することができる。
【０６３３】
この様に、図１５０の情報流通システムは、ポイント方式を採用するにあたり、そのポイントの不正利用に対処しシステムの安全性を向上させるとともに、利用者の便宜を殆ど損なう事が無い。ポイント方式の利用が制限されるのは新規入会時のみであり、以後はポイント方式とライセンス方式の両方式が利用可能である。すなわち、会員カード７１０２にライセンス情報とポイント情報のいずれか一方が記録される場合もあるし、双方が共に記録される場合もある。後者の場合は、ライセンス情報を優先的に用いることが望ましい。
【０６３４】
以下、図１５１を参照して、レンタルサービス提供のために、ディスク７１０３、会員カード７１０２、再生装置７１０１のそれぞれにおいて用いられる情報データについて説明する。
【０６３５】
ディスク７１０３には、
・課金対象の著作物であるコンテンツ情報をタイトルキーＫＴで暗号化したもの（［コンテンツ情報］ＫＴ）

・コンテンツの識別情報（コンテンツＩＤ）
・タイトルキーＫＴをディスクキーＫＤで暗号化したもの（［ＫＴ］ＫＤ）
・ディスクキーＫＤをマスターキーＫＭで暗号化したもの（［ＫＤ］ＫＭ）をさらにレンタルキーＫＲで暗号化したもの（［［ＫＤ］ＫＭ］ＫＲ）
・レンタルキーＫＲを複数の暗号用ライセンスキー（公開鍵）ＫＬＰ（ｊ）（ｊ＝１、２、３…）のそれぞれで暗号化したもの（［ＫＲ］ＫＬＰ（１）、［ＫＲ］ＫＬＰ（２）、［ＫＲ］ＫＬＰ（３）、…）
タイトルキーＫＴは、コンテンツ情報の１タイトル毎に予め定められた暗号鍵である。
【０６３６】
ディスクキーＫＤは、各ディスク毎に定められた暗号鍵である。
【０６３７】
マスターキーＫＭは、当該サービスに加入している会員にのみに与えられる暗号化復号化鍵で、図１５２の再生装置７１０１の第３の復号部７１０１ｉに格納されている。
【０６３８】
レンタルキーＫＲは、コンテンツ情報を復号する際に必要となる暗号化復号化鍵で、例えば、同時期に製造されたディスク７１０３には同一のレンタルキーが用いられる。
【０６３９】
暗号用ライセンスキーＫＬＰ（１）、ＫＬＰ（２）、ＫＬＰ（３）、…のそれぞれに対応する復号用ライセンスキーＫＬＳ（ｊ）は、レンタル時に会員カード７１０２に記録されるポイント情報に含まれている。
【０６４０】
異なる複数の暗号用ライセンスキーＫＬＰ（１）、ＫＬＰ（２）、ＫＬＰ（３）、…によって、レンタルキーＫＲを暗号化したものが複数ディスク７１０３に記録されているのは、適宜復号用ライセンスキーＫＬＳ（ｊ）を変更する事を可能にする為である。暗号用ライセンスキーＫＬＰ（ｊ）によって暗号化されたレンタルキーＫＲは、復号用ライセンスキーＫＬＳ（ｊ）によって復号することができる。
【０６４１】
ライセンス情報（ＣＬ）は、他の実施形態で述べたライセンス情報と同様で、例えば、レンタルキーＫＲ、ライセンス情報作成日時、利用条件等がマージされ、その全体が暗号化鍵Ｋｓで暗号化されている。すなわち、
暗号化ライセンス情報（［ＣＬ］Ｋｓ）＝［レンタルキーＫＲ＋ライセンス情報作成日時＋利用条件］Ｋｓ
と表すことができる。ライセンス情報（ＣＰ）は、会員カードに複数記録されている事もある。
【０６４２】
ポイント情報は、
・ポイントと認証情報Ａｐとをマージしたものを暗号鍵Ｋｔで暗号化したもの（［ポイント＋Ａｐ］Ｋｔ）
・複数の復号用レンタルキーＫＬＳ（ｊ）のうちの１つと、その識別子ｊとをマージし、全体を暗号化鍵ｋｓで暗号化されている。すなわち、
暗号化ポイント情報（［ＣＰ］Ｋｓ）＝［［ポイント＋Ａｐ］Ｋｔ＋ｊ＋ＫＬＳ（ｊ）］Ｋｓ
と表すことができる。
【０６４３】
暗号鍵ｋｔは、再生装置７１０１（図１５２の一時鍵発生部７１０１ｆ）にて発生される暗号鍵で、当該再生装置７１０１を一意的に特定でき、しかも、一度限り使用する（ここでは、１つのポイント情報を作成する際に用いられる）情報Ｒに相当するものである。すなわち、異なる再生装置からは異なる暗号鍵ｋｔが発生する。従って、［ポイント＋Ａｐ］Ｋｔを復号するには、当該暗号鍵ｋｔを発生した再生装置のみが行える。
【０６４４】

認証情報Ａｐは、当該ポイント情報が正当なものであるか否か（センター装置７１２１にて発行されたものであるか否か）を判断するための認証情報で、これと同一の認証情報は、再生装置７１２１の第２の復号部７１０１ｄに予め格納されていて、ポイント情報に含まれている認証情報Ａｐと照合を行うようになっている。

【０６４５】

なお、ライセンス情報、ポイント情報の表記で用いた記号「＋」は、情報がマージされることを示している。マージの際は、単にビット列を繋ぐだけでなく、予め定められた適当な方法でビット撹乱を施しても良い。

【０６４６】

暗号化鍵Ｋｓは、図１５０のセンター装置７１２１が保持し、暗号化鍵Ｋｓに対応する復号化鍵ｋｐは、再生装置７１０１（図１５２の鍵格納部７１０１ｃ）が保持している。

【０６４７】

第３の復号部７１０１ｉに格納されているマスターキーＫＭ、鍵格納部７１０１ｃに格納されている復号化鍵Ｋｐ、第２の復号部７１０１ｄに格納されている認証情報Ａｐは、当該レンタルサービスの加入時に各会員に渡される会員カード７１０２に予め記憶され、当該会員カード７１０２を当該会員の利用する再生装置に挿入されたときに読み取り、第３の復号部７１０１ｉ、鍵格納部７１０１ｃ、第２の復号部７１０１ｄに格納するようになっていてもよい。なお、再生装置７１０１によりマスターキーＫＭ、復号化鍵Ｋｐ、認証情報Ａｐが読み取られた後は、会員カード７１０２に記録されているマスターキーＫＭ、復号化鍵Ｋｐ、認証情報Ａｐは消去されることが望ましい。

【０６４８】

会員カード７１０２に記録されているライセンス情報を用いる場合、再生装置７１０１でライセンス情報に含まれる利用条件等に基づき当該ライセンスが有効であると判断されると、レンタルキーＫＲを得ることができるので、このレンタルキーＫＲを用いて［［ＫＤ］ＫＭ］ＫＲを復号し、［ＫＤ］ＫＭを得る。さらに、第３の復号部７１０１ｉに格納されているマスターキーＫＭを用いてディスクキーＫＤを得る。このディスクキーＫＤを用いて［ＫＴ］ＫＤを復号し、タイトルキーＫＴを得ることができる。

【０６４９】

会員カード７１０２に記録されているポイント情報を用いる場合、再生装置７１０１でポイント情報に含まれる［ポイント＋Ａｐ］Ｋｔを当該再生装置７１０１で発生し、一時鍵格納部７１０１ｅに予め格納されている暗号鍵Ｋｔにて復号し、ポイントと認証情報Ａｐを得る。認証情報Ａｐの照合とポイントの減算処理とを行った後、復号用ライセンスキーＫＬＳ（ｊ）を用いて［ＫＲ］ＫＬＰ（ｊ）を復号し、レンタルキーＫＲを得る。以後の処理は、ライセンス情報を用いた場合と同様である。

（１）再生装置

図１５２は、再生装置７１０１の構成例を示したもので、会員カード７１０２が挿入されて会員カード７１０２から各種情報データを読み取り、また、各種情報データを書き込むカード入出力部７１０１ａ、ポイント情報やライセンス情報を鍵格納部７１０１ｃに格納されている復号化鍵Ｋｐを用いて復号する第１の復号部７１０１ｂ、暗号鍵Ｋｔを発生する一時鍵発生部７１０１ｆ、一時鍵発生部７１０１ｆで発生した暗号鍵Ｋｔを一時格納する一時鍵格納部７１０１ｅ、ポイント情報に含まれている［ポイント＋Ａｐ］Ｋｔを一時鍵格納部７１０１ｅに一時格納されている暗号鍵Ｋｔを用いて復号し、認証情報Ａｐを照合する第２の復号部７１０１ｄ、ポイントを格納するポイント格納部７１０１ｇ、ライセンス情報に基づきそのライセンスの有効性を判定し、当該ライセンスが有効と判定されたときレンタルキーＫＲを第３の復号部７１０１ｉへ出力する判定部７１０１ｈ、コンテンツ情報の利用に応じてポイント格納部７１０１ｇに格納されているポイントの減算処理を行うポイント判定部７１０１ｊ、メディア読取部７１０１ｍでディスク７１０３から読み取られた情報と判定部７１０１ｈあるいはポイント判定部７１０１ｊから送られてきた情報とに基づきコンテンツ情報を復号する第３の復号部７１０１ｉ、第３の復号部７１０１ｉで復号されたコンテンツ情報を表示する表示部７１０１ｋ、ポイントの利用の可否等の

各種メッセージの提示やユーザからの指示入力を受け付けるためのユーザインタフェース７１０１１から構成されている。

【０６５０】

次に、図１５３に示すフローチャートを参照して図１５２の再生装置７１０１の処理動作の概略を説明する。

【０６５１】

入会時には会員カード７１０２には暗号化ライセンス情報（［ＣＰ］Ｋｓ）のみが記録されており、２回目以降のレンタル時には、暗号化ライセンス情報および暗号化ポイント情報（［ＣＰ］Ｋｓ）のうちの少なくとも１つが記録されている。

【０６５２】

ユーザは、会員カード７１０２を再生装置７１０１に挿入すると、カード入出力部７１０１ａは、当該会員カード７１０２から暗号化ポイント情報（［ＣＰ］Ｋｓ）の読み出しを行う（ステップＳ７１０１）。

【０６５３】

暗号化ポイント情報の読み出しに成功すると（ステップＳ７１０２）、当該再生装置７１０１のポイント格納部７１０１ｇに既に格納されているポイントに会員カード７１０２から読み出されたポイント情報に含まれるポイントを加算するポイント加算処理を実行する（ステップＳ７１０３）。

【０６５４】

次に、カード入出力部７１０１ａは、当該会員カード７１０２から暗号化ライセンス情報（［ＣＬ］Ｋｓ）の読み出しを行う（ステップＳ７１０４）。

【０６５５】

暗号化ライセンス情報の読み出しに成功すると（ステップＳ７１０５）、当該ライセンス情報に基づくライセンス判定処理を実行する（ステップＳ７１０６）。ライセンス判定処理では、ライセンス情報に基づくライセンス判定とコンテンツ情報の復号、再生を行う。一方、暗号化ライセンス情報が読み出せなかったとき（会員カード７１０２に暗号化ライセンス情報が記録されていないとき）は、ポイント格納部７１０１ｇに既に格納されているポイントを用いたコンテンツ情報利用に対する課金処理（ポイントの減算）、およびコンテンツ情報の復号、再生を行う（ステップＳ７１０７）。

【０６５６】

最後に、一時鍵発生部７１０１ｆは、暗号化鍵ｋｔを新たに発生し、一時鍵格納部７１０１ｅに格納し、会員カード７１０２に記録する等のＫｔの更新処理を実行する（ステップＳ７１０８）。ステップＳ７１０８のＫｔの更新処理は、図１５３に示した処理動作を行う度に、すなわち、コンテンツの再生を行う度に実行される。

【０６５７】

以上の処理動作では、会員カード７１０２に暗号化ライセンス情報が記録されている場合には、ライセンス情報を優先して用いている（ステップＳ７１０５）。また、会員カード７１０２に暗号化ポイント情報が記録されている場合、その暗号化ポイント情報が記録されてから最初に読み出した正当な再生装置（暗号化ポイント情報の復号に必要な暗号鍵ｋｔの発生元の再生装置）のみにしか、当該ポイントは利用できないようになっている。すなわち、ステップＳ７１０８のＫｔ更新処理では、会員カード７１０２に記録された暗号鍵Ｋｔを用いて暗号化ポイント情報が作成され、会員カード７１０２に記録されている。従って、ポイント利用範囲を当該暗号鍵ｋｔを発生した再生装置のみに限定することができたわけである。

【０６５８】

なお、第３の復号部７１０１ｉに格納されているマスターキーＫＭ、鍵格納部７１０１ｃに格納されている復号化鍵Ｋｐ、第２の復号部７１０１ｄに格納されている認証情報Ａｐを更新する際には、ユーザが店舗に赴きディスクのレンタルを行った際に、更新情報をそのまま、あるいは、所定の暗号鍵で暗号化して会員カード７１０２に記録しておく。当該会員カード７１０２をユーザが再生装置に挿入した際に、再生装置７１０１は図１５３に

示したような処理動作を実行する前に、会員カード７１０２から当該更新情報を読み出して、所定の更新処理を実行するようにしてもよい。

【０６５９】

次に、図１５４に示すフローチャートを参照して図１５３のステップＳ７１０３におけるポイント加算処理についてより詳細に説明する。

【０６６０】

ステップＳ７１０１で、カード入出力部７１０１ａにて会員カード７１０２から読み取られた暗号化ポイント情報（［ＣＰ］Ｋｓ）は、第１の復号部７１０１ｂに転送される。第１の復号部７１０１ｂは、鍵格納部７１０１ｃに予め格納されている復号化鍵Ｋｐを用いてポイント情報を復号する（ステップＳ７１１１）。復号されたポイント情報に含まれる情報データのうち、［ポイント＋Ａｐ］Ｋｔを第２の復号部７１０１ｄに転送する。

【０６６１】

第２の復号部７１０１ｄでは、一時鍵格納部７１０１ｅに格納されている暗号鍵Ｋｔを用いて、［ポイント＋Ａｐ］Ｋｔを復号し、ポイントと認証情報Ａｐとを得る（ステップＳ７１１２）。そして、このポイント情報に含まれていた認証情報Ａｐと第２の復号部７１０１ｂに既に格納されていた認証情報Ａｐとを照合し、一致していたら、第２の復号部７１０１ｄはポイント格納部７１０１ｇからそこに既に格納されているポイントを読み出して、それに、ポイント情報に含まれていたポイントを加算し、加算結果を再び、ポイント格納部７１０１ｇに格納する（ステップＳ７１１３～ステップＳ７１１６）。

【０６６２】

ここで、Ｋｔは、図１５３の処理動作を実行する度に更新されるとする。この場合、会員カード７１０２に記録された暗号化ポイント情報は、一度、図１５３に示したように再生装置７１０１に読み出された後は、ステップＳ７１０８にてＫｔが更新されるので、２度目に会員カード７１０２に記録された暗号化ポイント情報を読み出した際には、当該暗号化ポイント情報を作成する際に用いられたＫｔと再生装置７１０１にて保持されているＫｔとは異なるので、正常に［ポイント＋Ａｐ］Ｋｔを復号することができない。すなわち、ステップＳ７１１３において、当該ポイント情報に含まれていた認証情報Ａｐと第２の復号部７１０１ｂに既に格納されていた認証情報Ａｐとは不一致となるので、この場合は、ポイント加算処理を中止して、図１５３のステップＳ７１０４の処理に移る。

【０６６３】

次に、図１５５に示すフローチャートを参照して、図１５３のステップＳ７１０６におけるライセンス判定処理について説明する。

【０６６４】

ステップＳ７１０４で、カード入出力部７１０１ａにて会員カード７１０２から読み取られた暗号化ライセンス情報（［ＣＬ］Ｋｓ）は、第１の復号部７１０１ｂに転送される。第１の復号部７１０１ｂは、鍵格納部７１０１ｃに予め格納されている復号化鍵Ｋｐを用いてライセンス情報を復号する（ステップＳ７１２１）。復号されたライセンス情報は判定部７１０１ｈへ転送され、ここで、ライセンス情報に含まれる利用条件等に基づき、前述の実施形態で説明したきたような当該ライセンスの有効性を判定する（ステップＳ７１２２）。

【０６６５】

当該ライセンスが有効と判定されたとき、判定部７１０１ｈは当該ライセンス情報に含まれているレンタルキーＫＲを第３の復号部７１０１ｉへ転送する（ステップＳ７１２４）。

【０６６６】

第３の復号部７１０１ｉは、レンタルキーＫＲと、メディア読取部７１０１ｍにてディスク７１０３から読み取られた情報データ（［コンテンツ情報］ＫＴ、［ＫＴ］ＫＤ、［［ＫＤ］ＫＭ］ＫＲ）とを用いてコンテンツ情報を復号する。すなわち、レンタルキーＫＲを用いて［［ＫＤ］ＫＭ］ＫＲを復号し、［ＫＤ］ＫＭを得る。さらに、第３の復号部７１０１ｉに格納されているマスターキーＫＭを用いてディスクキーＫＤを得る。このディ

スクキーＫＤを用いて［ＫＴ］ＫＤを復号し、タイトルキーＫＴを得ることができる。このタイトルキーＫＴを用いてコンテンツ情報を復号し、表示部７１０１ｋに再生表示する（ステップＳ７１２５）。

【０６６７】

一方、ステップＳ７１２３で、当該ライセンスが無効（例えば、有効期限切れ）と判定されたときは、カード入出力部７１０１ａは、会員カード７１０２から暗号化ライセンス情報を消去し（ステップＳ７１２６）、ステップＳ７１０７と同様なポイント減算処理を実行する（ステップＳ７１２７）。

【０６６８】

次に、図１５６に示すフローチャートを参照して図１５３のステップＳ７１０７および図１５５のステップＳ７１２７におけるポイント減算処理について詳細に説明する。

【０６６９】

図１５４のステップＳ７１１１において、第１の復号部７１０１ｂで復号されたポイント情報に含まれていた復号用ライセンスキーＫＬＳ（ｊ）と、その識別子ｊは、ポイント判定部７１０１ｊに転送される（ステップＳ７１３１）。なお、課金カード７１０２に記録された当該暗号化ポイント情報の２度目以降の読み込みの際には、前述したように、当該暗号化ポイント情報を作成する際に用いた暗号鍵Ｋｔと、再生装置７１０１の一時鍵格納部７１０１ｅに格納されている暗号鍵Ｋｔとは異なる為、図１５４のステップＳ７１１２以降の処理は、常にステップＳ７１１３にて終了することとなる。従って、ポイント情報を用いコンテンツ復号動作は、図１５４のステップＳ７１１１から図１５６のポイント減算処理へ進むこととなる。

【０６７０】

ポイント判定部７１０１ｊは、ポイント格納部７１０１ｇからポイントを読み出し、当該コンテンツ情報の利用に応じたポイント値（例えば「１」）を減算する。なお、コンテンツ情報の１回の利用（再生）に対し予め定められたポイント値（例えば「１」）を交換する場合に限らず、例えば、ディスク７１０２に当該ディスク７１０２に記録されているコンテンツ情報の利用に対し差し引くべきポイント値が予め記録されており、これを読み出して、ポイントの減算処理を行うようにしてもよい。あるいは、コンテンツ情報の制作年月日が古いものほど差し引くべきポイントの値を小さくするようにしてもよい。この場合、図１５２のポイント判定部７１０１ｊは、制作年月日からの経過日数に応じて予め定められた差し引くべきポイント値のリストを保持していて、ディスク７１０２に記録された当該コンテンツ情報の制作年月日を読み取り、当該リストを参照して、差し引くべきポイント値を決定する。ポイント判定部７１０１ｊが保持するリストは、会員カード７１０２（あるいは、再生装置７１０１がセンター装置７１２１とオンライン接続されている場合には通信回線）を経由して更新される。

【０６７１】

さて、ステップＳ７１３３で得られたポイントの減算結果は負であったときは、そのまま処理動作を中断する（コンテンツ情報の再生は行わない）。

【０６７２】

減算結果が正であるときは、ユーザインタフェース７００１ｌにポイントの利用の有無を尋ねるメッセージを表示することが望ましい（ステップＳ７１３５）。このメッセージを見たユーザによりポイントの利用が指示されたときは（ステップＳ７１３６）、減算結果をポイント格納部７１０１ｇに格納する（ステップＳ７１３７）。すなわち、ポイント値を更新する。さらに、ポイント判定部７１０１ｇは、復号用ライセンスキーＫＬＳ（ｊ）と、その識別子ｊとを第３の復号部７１０１ｉに転送する（ステップＳ７１３８）。

【０６７３】

一方、メディア読取部７１０１ｍは、ディスク７１０３から情報データ（［ＫＲ］ＫＬＰ（ｊ）（ｊ＝１、２、３、…））を読み取り、第３の復号部７１０１ｉに転送する（ステップＳ７１３９）。

【０６７４】

第３の復号部７１０１ｉは、識別子ｊに対応する暗号用ライセンスキーＫＬＰ（ｊ）で暗号化されたレンタルキーＫＲ、すなわち、［ＫＲ］ＫＬＰ（ｊ）を選択して、それをポイント情報に含まれていた復号用ライセンスキーＫＬＳ（ｊ）を用いて復号し、レンタルキーＫＲを得る（ステップＳ７１４０）。

【０６７５】

メディア読取部７１０１ｍは、ディスク７１０３から情報データ（［コンテンツ情報］ＫＴ、［ＫＴ］ＫＤ、［［ＫＤ］ＫＭ］ＫＲ）を読み取り、第３の復号部７１０１ｉに転送する。第３の復号部７１０１ｉは、レンタルキーＫＲを用いて［［ＫＤ］ＫＭ］ＫＲを復号し、［ＫＤ］ＫＭを得る。さらに、第３の復号部７１０１ｉに格納されているマスターキーＫＭを用いてディスクキーＫＤを得る。このディスクキーＫＤを用いて［ＫＴ］ＫＤを復号し、タイトルキーＫＴを得ることができる。このタイトルキーＫＴを用いてコンテンツ情報を復号し、表示部７１０１ｋに再生表示する（ステップＳ７１４１）。

【０６７６】

次に、図１５７に示すフローチャートを参照して図１５５のステップＳ７１２５および図１５６のステップＳ７１４１におけるコンテンツ表示処理について詳細に説明する。

【０６７７】

メディア読取部７１０１ｍは、ディスク７１０３から情報データ（［ＫＴ］ＫＤ、［［ＫＤ］ＫＭ］ＫＲ）を読み取り、第３の復号部７１０１ｉに転送する（ステップＳ７１５１）。第３の復号部７１０１ｉは、レンタルキーＫＲを用いて［［ＫＤ］ＫＭ］ＫＲを復号し、［ＫＤ］ＫＭを得る。さらに、第３の復号部７１０１ｉに格納されているマスターキーＫＭを用いてディスクキーＫＤを得る。このディスクキーＫＤを用いて［ＫＴ］ＫＤを復号し、タイトルキーＫＴを得ることができる（ステップＳ７１５２）。

【０６７８】

メディア読取部７１０１ｍは、ディスク７１０３から暗号化コンテンツ情報［コンテンツ情報］ＫＴを読み取り、第３の復号部７１０１ｉに転送する（ステップＳ７１５３）。第３の復号部７１０１ｉは、タイトルキーＫＴを用いてコンテンツ情報を復号し（ステップＳ７１５４）、表示部７１０１ｋに再生表示する（ステップＳ７１５５）。

【０６７９】

次に、図１５３のステップＳ７１０８の暗号鍵Ｋｔの更新処理について、図１５８に示すフローチャートを参照して説明する。

【０６８０】

例えば、ポイント情報あるいはライセンス情報を用いたコンテンツの表示処理が終了した後、図１５５のステップＳ７１２３でライセンスが無効と判断されたとき、図１５６のステップＳ７１３４でポイントの使いきりが検知されたとき、一時鍵生成部７１０１ｆは、暗号鍵ｋｔを生成する（ステップＳ７１６１）。なお、暗号鍵生成方法は、ここでは、特に限定しない。

【０６８１】

一時鍵発生部７１０１ｆで生成された暗号鍵Ｋｔは一時鍵格納部７１０１ｅに格納され（ステップＳ７１６２）、さらにカード入出力部７１０１ａから会員カード７１０２に当該更新された暗号鍵Ｋｔが書き込まれる（ステップＳ７１６３）。

（２）ライセンス／ポイント注入装置

図１５９は、ライセンス／ポイント注入装置７１１１の構成例を示したもので、センター装置７１２１に接続して、ライセンス情報／ポイント情報の発行要求を送信したり、当該要求に応じてセンター装置７１２１から発行されライセンス情報／ポイント情報を受信するための通信部７１１１ａ、会員カード７１０２が挿入されて会員カード７１０２から各種情報データを読み取り、また、各種情報データを書き込むカード入出力部７１１１ｃ、ディスク７１０３から各種情報データを読み出すためのメディア読取部７１１１ｅ、ライセンス情報にマージされる利用条件や、ポイント情報にマージされるポイント等の情報データを入力するための条件入力部７１１１ｄ、上記各部を制御する制御部７１１１ｂから構成されている。

【０６８２】
次に、図１６０、図１６１に示すフローチャートを参照して図１５９のライセンス／ポイント注入装置７１１１の処理動作の概略を説明する。
【０６８３】
まず、図１６０を参照して、ライセンス情報発行処理動作について説明する。
例えば店舗の店員が当該レンタルサービスの会員の会員カード７１０２をカード入出力部７１１１ｃに挿入し、当該会員により選択されたディスク７１０３をメディア読取部７１１１ｅにセットする。店員は、条件入出力部７１１１ｄから当該ディスク７１０３に記録されているコンテンツ情報に対する利用条件等を入力し、ライセンス情報発行要求の指示入力を行うと（ステップＳ７１７１）、メディア読取部７１１１ｅは、ディスク７１０３からコンテンツＩＤを読み取る（ステップＳ７１７２）。制御部７１１１ｂは、通信部７１１１ａを介してセンター装置７１２１へ、コンテンツの利用条件、コンテンツＩＤを含むライセンス情報の発行要求を送信する（ステップＳ７１７３）。
【０６８４】
ライセンス情報の発行要求を受けてセンター装置７１２１にて発行された暗号化ライセンス情報（［ＣＬ］Ｋｓ）は、通信部７１１１ａで受信される（ステップＳ７１７４）。制御部７１１１ｂは、通信部７１１１ａで受信された暗号化ライセンス情報をカード入出力部７１１１ｃへ転送し、カード入出力部７１１１ｃは、当該暗号化ライセンス情報を会員カード７１０２に記録する（ステップＳ７１７５）。
【０６８５】
次に、図１６１を参照して、ポイント情報発行処理動作について説明する。
【０６８６】
例えば店舗の店員が当該レンタルサービスの会員の会員カード７１０２をカード入出力部７１１１ｃに挿入する。店員は、条件入出力部７１１１ｄから購入されたポイントを入力し、ポイント情報発行要求の指示入力を行うと（ステップＳ７１８１）、カード入出力部７１１１ｃは、会員カード７１０２から暗号化ポイント情報を読み取る（ステップＳ７１８２）。ここで、読み取られた暗号化ポイント情報は、消去してもよい。
【０６８７】
次に、カード入出力部７１１１ｃは会員カード７１０２から暗号鍵Ｋｔを読み取る（ステップＳ７１８３）。暗号鍵Ｋｔを読み取ることができなかったときは、ポイント情報の発行ができないので、処理を中断する。
【０６８８】
一方、暗号鍵Ｋｔの読み取りに成功した場合は（ステップＳ７１８４）、制御部７１１１ｂは、通信部７１１１ａを介してセンター装置７１２１へポイント値、暗号鍵Ｋｔを含むポイント情報の発行要求を送信する（ステップＳ７１８５）。
【０６８９】
ポイント情報の発行要求を受けてセンター装置７１２１にて発行された暗号化ポイント情報（［ＣＰ］Ｋｓ）は、通信部７１１１ａで受信される（ステップＳ７１８６）。制御部７１１１ｂは、通信部７１１１ａで受信された暗号化ポイント情報をカード入出力部７１１１ｃへ転送し、カード入出力部７１１１ｃは、当該暗号化ポイント情報を会員カード７１０２に記録する（ステップＳ７１８７）。
（３）センター装置
図１６２は、センター装置７１２１の構成例を示したもので、第１の暗号化部７１２１ａ、第２の暗号化部７１２１ｂ、鍵格納部７１２１ｃ、認証情報格納部７１２１ｄ、ライセンスキー格納部７１２１ｅ、通信部７１２１ｆ、コンテンツデータベース７０２１ｇ、時計７０２１ｈから構成されている。
【０６９０】
コンテンツデータベース７０２１ｇには、コンテンツＩＤに対応させて、レンタルキーＫＲが記憶されている。
【０６９１】

鍵格納部７１２１ｃには、ライセンス情報とポイント情報を暗号化するための暗号鍵Ｋｓが格納されている。

【０６９２】

認証情報格納部７１２１ｄには、認証情報Ａｐが格納されている。

【０６９３】

ライセンスキー格納部７１２１ｅには、復号用ライセンスキーＫＬＳ（ｊ）（ｊ＝１、２、３、…）が格納されている。

【０６９４】

通信部７１２１ｆは、ライセンス／ポイント注入装置７１１１に接続して、ライセンス情報／ポイント情報の発行要求を受信したり、当該要求に応じて発行したライセンス情報／ポイント情報をライセンス／ポイント注入装置７１１１に送信する。

【０６９５】

次に、図１６３、図１６４に示すフローチャートを参照して図１６２のセンター装置７１２１の処理動作の概略を説明する。

【０６９６】

まず、図１６３を参照して、ライセンス情報発行処理動作について説明する。

通信部７１２１ｆは、ライセンス／ポイント注入装置７１１１から、コンテンツの利用条件、コンテンツＩＤを含むライセンス情報の発行要求を受信すると（ステップＳ７１９１）、第１の暗号化部７１２ａへコンテンツＩＤと利用条件等を転送する（ステップＳ７１９２）。

【０６９７】

第１の暗号化部７１２１ａは、コンテンツデータベース７０２１ｇから当該コンテンツＩＤに対応するレンタルキーＫＲを読み出し（ステップＳ７１９３）、時計７０２１ｈから現在日時を読み出し（ステップＳ７１９４）、さらに、鍵格納部７１２１ｃから暗号鍵Ｋｓを読み出し、暗号化ライセンス情報［ＣＬ］Ｋｓ＝［ＫＲ＋ライセンス情報作成日時＋利用条件］Ｋｓを作成する（ステップＳ７１９５）。

【０６９８】

通信部７１２１ｆは、第１の暗号化部７１２１ａで作成された暗号化ライセンス情報をライセンス／ポイント注入装置７１１１へ送信する（ステップＳ７１９６）。

【０６９９】

図１６４に示すフローチャートを参照して、ポイント情報発行処理動作について説明する。

【０７００】

通信部７１２１ｆは、ライセンス／ポイント注入装置７１１１から、ポイント値と暗号鍵Ｋｔを含むポイント情報の発行要求を受信すると（ステップＳ７２０１）、第２の暗号化部７１２１ｂへポイント値と暗号鍵Ｋｔとを転送する（ステップＳ７２０２）。

【０７０１】

第２の暗号化部７１２１ｂは、認証情報格納部７１２１ｄから認証情報Ａｐをを読み出し（ステップＳ７２０３）、当該認証情報とポイント情報とをマージして、さらに暗号鍵Ｋｔで暗号化し、［ポイント情報＋Ａｐ］Ｋｔを生成する（ステップＳ７２０４）。

【０７０２】

第１の暗号化部７１２１ａは、ライセンスキー格納部７１２１ｅから復号用ライセンスキーＫＬＳ（ｊ）とその識別子ｊを１組読み出し（ステップＳ７２０５）、［ポイント情報＋Ａｐ］Ｋｔと復号用ライセンスキーＫＬＳ（ｊ）とその識別子ｊとをマージして、さらに、鍵格納部７１２１ｃから読み出された暗号鍵ｋｓで暗号化して、暗号化ポイント情報［ＣＰ］Ｋｓ＝［［ポイント情報＋Ａｐ］Ｋｔ＋復号用ライセンスキーＫＬＳ（ｊ）＋ｊ］Ｋｓを作成する（ステップＳ７２０６）。

【０７０３】

通信部７１２１ｆは、第１の暗号化部７１２１ａで作成された暗号化ポイント情報をライセンス／ポイント注入装置７１１１へ送信する（ステップＳ７２０７）。

【０７０４】
なお、上記実施形態において、再生装置７１０１の購入時（当該レンタルサービス入会時）に、例えば店舗にて、あるいは、再生装置７１０１の製造時に、第３の復号部７１０１ｉ、鍵格納部７１０１ｃ、第２の復号部７１０１ｄにそれぞれ、マスターキーＫＭ、復号化鍵Ｋｐ、認証情報Ａｐを書き込むようにしてもよい。
【０７０５】
また、例えば、当該レンタルサービス入会時に購入した再生装置７１０１にはそれに対応した会員カード７１０２が添付されており、この会員カード７１０２には、既に再生装置７１０１にて発生された暗号鍵Ｋｔが書き込まれているものであってもよい。この場合、上記実施形態では、初回目は必ずライセンス情報を用いなければならなかったが、レンタルサービス入会時には、既に会員カード７１０２に再生装置７１０１にて発生されｔ暗号鍵Ｋｔが書き込まれているので、当該レンタルサービス入会と同時にポイント情報を用いたコンテンツ再生が行えるようになる。
【０７０６】
また、上記実施形態では、会員の利用する再生装置７１０１から発生される暗号鍵Ｋｔを用いて暗号化ポイント情報を作成することにより、当該会員により購入されたポイントの使用を当該会員の使用する再生装置７１０１のみに限定するものであったが、この場合に限らず、さらに、当該ポイントの利用を特定のコンテンツ（あるいは特定のカテゴリーのコンテンツ）に限定することも可能である（例えば、未成年者には視聴可能なカテゴリーを限定することができる）。この場合、例えば、暗号用ライセンスキーＫＬＰ（１）、ＫＬＰ（２）、ＫＬＰ（３）、…を用いることにより、レンタル業者側から（必要があれば、会員に知られることなく）操作することができる。すなわち、例えば、会員により購入されたポイントの利用を特定のカテゴリーに属するコンテンツの再生のみに限定する場合には、当該購入されたポイントを含む暗号化ポイント情報には、複数の復号用ライセンスキーのうち、当該限定したいカテゴリーに対し予め割り当てられた復号用ライセンスキーＫＬＳ（ｊ）のみが含まれていればよい。もちろん、ディスク７１０３には、そこに記録されているコンテンツのカテゴリーに応じた暗号用ライセンスキーＫＬＰ（ｊ）で暗号化されたレンタルキーＫＲのみが記録されている。
【０７０７】
以上説明したように、上記実施形態によれば、
・　会員が利用する再生装置で発生された各再生装置固有の暗号鍵Ｋｔを用いて暗号化ポイント情報を作成することにより、当該会員により購入されたポイントの利用を当該会員の利用する再生装置にのみに限定することができる。
【０７０８】
・　コンテンツのカテゴリー毎にライセンスキー（ＫＬＰ（ｊ）とＫＬＳ（ｊ））を定め、暗号化ポイント情報に当該会員に視聴可能なカテゴリーの復号用ライセンスキーＫＬＳ（ｊ）のみが含まれていることにより、また、貸し出されるディスクには、そこに記録されているコンテンツのカテゴリーに応じた暗号用ライセンスキーＫＬＰ（ｊ）で暗号化されたレンタルキーＫＲのみが記録されていることにより、会員により購入されたポイントの利用を、当該会員が視聴可能なカテゴリーのコンテンツの視聴にのみに限定することができる。
（４）　ポイントのみを用いたレンタルサービスの実施形態
以下、競合する複数のレンタル業者により提供される複数のレンタルサービスに１つの再生装置を用いる場合を例にとり説明する。
【０７０９】
上記した実施形態では、初回目は必ずライセンス情報を用いなければならなかったが、レンタルサービス入会時から、すなわち、初回目からライセンス情報を用いることなく、ポイントのみを用いたレンタルサービスを実現する方が再生装置の構成を簡略化する上で有効である（例えば、判定部７１０１でライセンス情報に含まれる利用条件（例えば期限）の有効性を判定するために必要な時計が不要となる）。

【０７１０】
そこで、入会直後の初回目のレンタル時に会員カード７１０２に書き込まれる初回暗号化ポイント情報［ＣＰ０］Ｋｓの構成を
初回暗号化ポイント情報（［ＣＰ０］Ｋｓ）＝［ポイント＋ｊ＋ＫＬＳ（ｊ）＋業者ＩＤ］Ｋｓとする。
【０７１１】
業者ＩＤとは、異なるレンタル業者のそれぞれを識別するためのＩＤであるとともに、ポイント格納部７１０１ｇへのポイント値の書込および読み出しを制御するために用いる情報である。
【０７１２】
また、ポイント格納部７１０１ｇには、レンタル業者毎に業者ＩＤとそのポイント値を書き込む領域がそれぞれ設けられていている。
【０７１３】
また、２回目以降にポイントを購入した際に作成される暗号化ポイント情報には、さらに業者ＩＤが含まれている。すなわち、ここで用いる暗号化ポイント情報［ＣＰ］Ｋｓ’は、
暗号化ポイント情報（［ＣＰ］Ｋｓ’）＝［［ポイント＋Ａｐ］Ｋｔ＋ｊ＋ＫＬＳ（ｊ）＋業者ＩＤ］Ｋｓ
と表すことができる。
【０７１４】
以下、再生装置７１０１の初回暗号化ポイント情報の処理動作について説明する。
【０７１５】
ステップＳ７３０１）　図１５３のステップＳ７１０１にて再生装置７１０１が会員カード７１０２から通常の暗号化ポイント情報（［ＣＰ］Ｋｓ’）を読み出す前に、上記初回暗号化ポイント情報［ＣＰ０］Ｋｓの読み出しを行う（会員カード７１０２には、［ＣＰ］Ｋｓ’と［ＣＰ０］Ｋｓの両方が書き込まれていてもよい）。
【０７１６】
ステップＳ７３０２）　カード入出力部７１０１ａで読み出された初回暗号化ポイント情報は、第１の復号部７１０１ｂへ転送され、第１の復号部７１０１ｂにて復号化鍵Ｋｐを用いて初回ポイント情報を復号し、その中に含まれている業者ＩＤ（例えば「ｘｘ」とする）と、ポイントを判定部７１０１ｈへ転送する。
判定部７１０１ｈは、ポイント格納部７１０１ｇから当該業者ＩＤ（ｘｘ）を検索し、ポイント格納部７１０１ｇに当該業者ＩＤ（ｘｘ）が未だ書き込まれていないときのみ、当該ポイント値を当該業者ＩＤ（ｘｘ）に対応させてポイント格納部７１０１ｇに書き込む。
【０７１７】
当該同一業者の初回暗号化ポイント情報を用いた２回目以降のコンテンツ再生時には、再び、上記処理（ステップＳ７３０１～ステップＳ７３０２）を実行することになるが、その場合には、ポイント格納部７１０１ｇに当該業者ＩＤ（ｘｘ）が既に書き込まれているので、再び、同じ初回暗号化ポイント情報によるポイントの書き込み（加算）は行うことなく、図１５３のステップＳ７１０１の処理に進む。
【０７１８】
一方、ステップＳ７３０１にて異なる業者（業者ＩＤ（ｙｙ））の初回暗号化ポイント情報を新たに読み出した場合、ポイント格納部７１０１ｇに、その業者ＩＤが存在しない限り、当該業者ＩＤ（ｙｙ）と、当該初回暗号化ポイント情報に含まれていたポイント値とをポイント格納部７１０１ｇに書き込む。
【０７１９】
以上の処理動作が、図１５３のステップＳ７１０１の前段に追加され、以後の処理動作は、前述同様である。すなわち、２回目以降のポイント購入時には、当該再生装置７１０１が発生した暗号鍵Ｋｔを用いて暗号化ポイント情報（［ＣＰ］Ｋｓ’）が作成される。

【０７２０】
異なるのは、２回目以降のポイントの購入時に作成される暗号化ポイント情報には前述したように、そのポイントを購入したレンタル業者のＩＤが含まれていて、図１５３～図１５８に示したような処理動作は、この業者ＩＤに対応してポイント格納部７１０１ｇに記録されたポイントが減算されることにより実行されることである。より詳しくは、図１５３のステップＳ７１０１～ステップＳ７１０３、ステップＳ７１０７～ステップＳ７１０８に対応する処理動作のみを行うことになる。
【０７２１】
暗号化ポイント情報［ＣＰ］Ｋｓ’に含まれる業者ＩＤの確認は、判定部７１０１ｈにて行うものとする。すなわち、図１５４のステップＳ７１１１において、暗号化ポイント情報［ＣＰ］Ｋｓ’を復号すると、その中に含まれていた業者ＩＤは判定部７１０１ｈに転送され、ステップＳ７１１６において、第２の復号部７１０１ｄがポイント格納部７１０１ｇにポイント値を書き込む際には、判定部７１０１ｈにて指示された業者ＩＤに対応するポイント書込領域に書き込む。また、図１５６のポイント減算処理のステップＳ７１３２、ステップＳ７１３７において、ポイント判定部７１０１ｊがポイント格納部７１０１ｇからポイントを読み書きする際には、判定部７１０１ｈにて指示された業者ＩＤに対応するポイント書込領域から当該ポイント値の読み出し／書き込みを行う。
【０７２２】
なお、レンタル業者が１つのみの場合も上記同様である。すなわち、業者ＩＤが１つのみしかこの世に存在しない場合も、入会直後からポイントを用いたレンタルサービスが実現できる。この場合、業者ＩＤとは、単に、初回にポイント格納部７１０１ｇへポイント値の書込みを制御するために用いるだけである。
【０７２３】
以上説明したように、暗号化ポイント情報は業者ＩＤを含み、初回のみ、業者ＩＤを用いてポイント格納部７１０１ｇへのポイント値の書込を制御することにより、ポイントのみを用いたレンタルサービスが容易に行える。
【０７２４】
また、ポイント格納部７１０１ｇには、業者ＩＤ毎にポイント書込領域が設けられていていて、暗号化ポイント情報に含まれている業者ＩＤに基づき、ポイント格納部７１０１ｇに格納されているポイントを減算することにより、１つの再生装置で複数の競合するレンタル業者のそれぞれにて販売されるポイントを利用することができる。この場合、貸し出されるディスクは複数のレンタル業者で共通したものであってもよいし、レンタル業者毎に異なっていてもよい。
（第７の実施形態）
（７－１）
図１６５は、本発明の第７の実施形態に係る情報流通システムに用いられる再生装置の構成例を示したもので、ＤＶＤ、ＣＤ、ＬＤ、ビデオテープ等の記録メディア（以下、簡単にメディアと呼ぶ）８００１からメディア記録情報を読み出すメディア読取部８１０２と、復号ユニット８１０３と、表示装置８１１２とから構成されている。
【０７２５】
メディア読取部８１０２は、メディア８１０１に対応した従来からある読取装置（例えばメディア８１０１がＤＶＤならばＤＶＤプレーヤ、ＣＤならＣＤプレーヤ）を用いる。
【０７２６】
ここでは、メディア８１０３に記録されている暗号化コンテンツ情報の利用に対する点数（ポイント）を予め購入して、メディア８１０３を貸し出すことによりなるレンタルサービスを提供するための再生装置について説明する。
【０７２７】
メディア８１０１には、図１６６に示すように、コンテンツキーＫｃで暗号化された課金対象のコンテンツ情報（暗号化コンテンツ情報）に、当該コンテンツキーＫｃをレンタルキーＫｒで暗号化して生成したＷＭ情報を電子すかし（Ｄｉｇｉｔａｌ　Ｗａｔｅｒｍａ

ｒｋ）技術で合成して得られるメディア記録情報が記録されている。
【０７２８】
ここで、「コンテンツ情報を暗号化する」とは、例えばコンテンツ情報が画像であれば、その輝度を変えるといった、当該コンテンツ情報に対しその実体が視聴者には明らかにならないように施す加工処理をも含むものである。従って、ここで、コンテンツキーＫｃとは、この加工処理を施されたコンテンツを復元するために必要な情報である。
【０７２９】
コンテンツキーＫｃは、コンテンツ情報の暗号化復号化鍵で、少なくともコンテンツのタイトル毎に異なっていることが望ましい。
【０７３０】
レンタルキーＫｒは、コンテンツキーの暗号化復号化鍵で、例えば、同時期に製造されたディスク７１０３には同一のレンタルキーが用いられる。
【０７３１】
WM情報の埋め込み位置としては、暗号化コンテンツ情報の全体に均一に、あるいは所定間隔毎に埋め込むようにしてもよし、図１７２に示すように、コンテンツ情報の先頭にある未暗号化部分に埋め込むようにしてもよい。この場合、コンテンツ情報に、WM情報が埋め込まれてなく、かつ、暗号化されていない領域（例えば、WN情報の処理時間相当分）Ｒ１００が存在していてもよい。なお、暗号化されていない領域Ｒ１００は、WM情報の埋め込み領域の前方にあってもよい。いずれにしても、当該WM情報の埋め込み位置は、暗号化コンテンツ情報の前方にあるべきである。
【０７３２】
コンテンツ情報の利用に対する予め購入されたポイントは、カード型記録媒体（以下、カードと呼ぶ）８０１０に記録されていて、カード８１１０は復号ユニット８１０３に挿入することにより、メディア８１０１に記録されているコンテンツ情報の再生が行えるようになっている。すなわち、メディア８１０１に記録されているコンテンツ情報を再生する度に当該コンテンツ情報に応じて所定値のポイントがカード８１１０に予め記録されているポイントが減算されていく。このポイント値がなくなると、コンテンツ情報の再生は行えない。
【０７３３】
カード８１１０には、少なくとも、支払った金額に応じたポイント値と、レンタルキーＫｒとが記録されている。ポイント値とレンタルキーＫｒはそのまま記録されていてもよいが、所定の加工処理（例えば、暗号化処理等）を施してから記録するようにしてもよい。
【０７３４】
レンタルキーＫｒは、レンタル時、あるいは、ポイント購入時にカード８１１０に記録されるものとしてもよい。
【０７３５】
以下、図１６７に示すフローチャートを参照して、図１６５の再生装置の処理動作について説明する。
【０７３６】
メディア読取部８１０２にメディア８１０１がセットされ、復号ユニット８１０３にカード８１１０が挿入されると、メディア８１０１に記録されたメディア記録情報（Ｃ’）は、メディア８１０１に対応した読取装置（例えばメディア８１０１がＤＶＤならばＤＶＤプレーヤ、ＣＤならＣＤプレーヤ）で読み取られ、復号ユニット８１０３へ出力される。メディア記録情報（Ｃ’）は、復号ユニット８１０３ののWM分離部８１０４に入力する（ステップＳ８１０１）。
【０７３７】
WM分離部８１０４は、入力したメディア記録情報（Ｃ’）を暗号化コンテンツ情報（Ｃ”）とWM情報（W）とに分離し、前者をコンテンツ復号部８１０８に、後者をWM格納部８１０５にそれぞれ転送する（ステップＳ８１０２、ステップＳ８１０３）。
【０７３８】

一方、ポイント減算部８１０９は、挿入されたカード８１１０からポイントを読み出し、当該ポイント値がこれから再生しようとするコンテンツ情報の利用に対するポイント値以上の値であるか（有効量であるか）否かを判断する。当該ポイント値が有効量（例えば、ポイント＞０）である判断すると、キー復号部８１０６を起動する。起動されたキー復号部８１０６は、WM格納部８１０５からWM情報を読み出す。さらに、ポイント減算部８１０９は、カード８１１０からレンタルキーＫｒを取得し、キー復号部８１０６へ転送する（ステップＳ８１０４～ステップＳ８１０６）。キー復号部８１０６は、レンタルキーＫｒを用いてWM情報からコンテンツキーＫｃを復号し、キー格納部５００７に格納する（ステップＳ８１０６～ステップＳ８１０７）。

【０７３９】

一方、コンテンツ復号部５００８は、WM分離部５００４から渡された暗号化コンテンツ情報（Ｃ”）をキー格納部５００７から読み出したコンテンツキーＫｃで復号してコンテンツ情報（Ｃ）を得、表示装置５０１１へ出力する（ステップＳ８１０９～ステップＳ８１１０）。

【０７４０】

ステップＳ８１０５で、カード８１１０のポイント値が有効量でないと判断されたとき、もしくは、ステップＳ８１０６でカード８１１０から出力されたレンタルキーがWM情報生成に用いたレンタルキーＫｒと相違していたときは、コンテンツ情報は正常に復号されず、利用者に提示されないことになる。

（７－２）

図１６８は、第７の実施形態に係る情報流通システムに用いられる再生装置の他の構成例を示したものである。なお、図１６５と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図１６５のメディア読取部８１０２が図１６８では、放送波受信部（チューナ）８０２１に置き換わっていて、図１６６に示したようなメディア記録情報が放送波として各ユーザ宅に配信されるようになっている。チューナ８０２１は、受信した放送波から抽出されたメディア記録情報（Ｃ’）を復号ユニット８１０３へ出力する。

（７－３）

メディア記録情報の他の例を図１７０を参照して説明する。図１６６に示したメディア記録情報と異なるのは、WM情報である。すなわち、図１７０では、１つのコンテンツキーＫｃを複数のレンタルキーＫｒ１、Ｋｒ２、…、Ｋｒｎで暗号化したものを結合（マージ）し、それをWM情報としている。

【０７４１】

図１７０に示したようなメディア記録情報を用いた再生装置の構成例を図１６９に示す。なお、図１６９において、図１６５と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、カード８１３０には、複数のレンタルキーレンタルキーＫｒ１、Ｋｒ２、…、Ｋｒｎのうちの１つ、あるいは複数、あるいは全てが記録されている。

【０７４２】

図１７１は、図１６９の再生装置の処理動作を説明するためのフローチャートである。なお、図１６７と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図１６７のス８００６とステップＳ８１０７が、図１７１ではステップＳ８１２１とステップＳ８１２２に置き換わっている。

【０７４３】

キー復号部８１３１は、カード８１３０から出力される複数のレンタルキーのうちの１つ（Ｋｒｉ）を用いてWM情報からコンテンツキーＫｃを得るようになっている。カード８１３０に複数のライセンスキーが記録されている場合は、それらを１つづつ読み出して、WM情報を復号していく。

【０７４４】

WM情報には、コンテンツキーの他に、正確に復号できたか否かをチェックするための予め仇米良れた認証情報が含まれいることが望ましい。この認証情報が正確に復号できたか

否かにより、正当なコンテンツキーが得られたか否かが容易に判断できる。
【０７４５】
ステップＳ８１０５で、カード８１１０のポイント値が有効量でないと判断されたとき、もしくは、ステップＳ８１２１でカード８１３０から出力されたレンタルキーがＷＭ情報生成に用いたレンタルキーＫｒ１、Ｋｒ２、…、Ｋｒｎのいずれとも合致しないときは、コンテンツ情報は正常に復号されず、利用者に提示されないことになる。
【０７４６】
【発明の効果】
以上説明したように、本発明の情報記録装置および情報再生装置およに課金装置によれば、ネットワークあるいは記録媒体を介して分配されたディジタル化された著作物を迅速かつ手軽に流通させるとともに、ディジタル情報の利用に対する課金による著作権の保護を前提としたディジタル情報の利用環境を容易に構築できる。
【図面の簡単な説明】
【図１】本発明の実施形態に係る情報記録装置の第１の構成例を示した図。
【図２】図１の第１の情報記録装置の動作を説明するためのフローチャート。
【図３】本発明の実施形態に係る情報記録装置の第２の構成例を示した図。
【図４】図３の第２の情報記録装置の動作を説明するためのフローチャート。
【図５】課金対象情報データの分離方法を説明するための図。
【図６】課金対象情報データの他の分離方法を説明するための図。
【図７】本発明の実施形態に係る情報記録装置の第３の構成例を示した図。
【図８】本発明の実施形態に係る情報再生装置の第１の構成例を示した図。
【図９】図８の復号ユニットの構成例を示した図。
【図１０】図８の第１の情報再生装置の動作を説明するためのフローチャート。
【図１１】図９の復号ユニットの動作を説明するためのフローチャート。
【図１２】復号ユニットの他の構成例を示した図で、時刻の更新を無効にする時計を具備した復号ユニットの場合を示している。
【図１３】復号ユニットに具備される時計の時刻の更新を無効にするための動作を説明するためのフローチャート。
【図１４】図１２の復号ユニットの動作を説明するためのフローチャート。
【図１５】時刻の更新が可能な復号ユニットに具備された時計の構成例を示した図。
【図１６】図１５の時計の時刻更新動作を説明するためのフローチャート。
【図１７】ネットワークを介して復号ユニットに具備された時計の時刻更新を行う場合のクライアントとサーバとで構成されるシステムの全体図。
【図１８】図１７の時刻設定クライアントの構成例を示した図。
【図１９】図１７の時刻設定サーバの構成例を示した図。
【図２０】図１８の時刻設定クライアントの動作を説明するためのフローチャート。
【図２１】図１９の時刻設定サーバの動作を説明するためのフローチャート。
【図２２】図１９の時刻設定サーバの動作を説明するためのフローチャート。
【図２３】図１８の時刻設定クライアントに具備される時計の構成例を示した図。
【図２４】図２３の時計の動作を説明するためのフローチャート。
【図２５】図２３の時計の動作を説明するためのフローチャート。
【図２６】ライセンス情報の更新および課金を行う機能を具備した情報再生装置（第２の情報再生装置）の構成例を示した図。
【図２７】図２６の復号ユニットの構成例を示した図。
【図２８】図２７の復号ユニットの動作を説明するためのフローチャート。
【図２９】図２６のライセンス情報更新クライアント部の構成例を示した図。
【図３０】図２９のライセンス情報更新クライアント部の動作を説明するためのフローチャート。
【図３１】図２６のライセンス情報更新サーバの構成例を示した図。
【図３２】図３１のライセンス情報更新サーバの動作を説明するためのフローチャート。

【図３３】ライセンス情報更新サーバから出力される課金対象情報の利用に対する料金の支払い要求の内容の一例を示した図。
【図３４】図２６のシステム全体（ネットワークを介し互いに通信を行うサーバおよびクライアント）の動作を説明するためのフローチャート。
【図３５】ライセンス情報更新ユニットの構成例を示した図。
【図３６】図３５のライセンス情報更新ユニットの動作を説明するためのフローチャート。
【図３７】図３５のライセンス情報更新ユニットの動作を説明するためのフローチャート。
【図３８】課金対象情報の利用に対する課金を行うための課金装置の構成例を示した図。
【図３９】課金対象情報の不正コピーの防止対策（復号ユニットＩＤに基づく判定を行う）を講じた情報再生装置の復号ユニットの構成例を示した図。
【図４０】図３９の動作を説明するためのフローチャート。
【図４１】課金対象情報の不正コピーの防止対策を講じたライセンス情報更新ユニットの構成例を示した図。
【図４２】図４１のライセンス情報更新ユニットの動作を説明するためのフローチャート。
【図４３】課金対象情報の不正コピーの防止対策を講じた（復号ユニットＩＤおよびメディアＩＤに基づく判定を行う）復号ユニットの他の構成例を示した図。
【図４４】図４３の復号ユニットの動作を説明するためのフローチャート。
【図４５】コピー装置の構成例を示した図。
【図４６】図４５のコピー装置の動作を説明するためのフローチャート。
【図４７】図４５のライセンス情報複製ユニットの構成例を示した図。
【図４８】図４７のライセンス情報複製ユニットの動作を説明するためのフローチャート。
【図４９】本発明の実施形態に係る副情報を再生する場合の情報再生装置（第３の情報再生装置）の構成例を示した図。
【図５０】図４９の第３の情報再生装置の構成例を示した図。
【図５１】図４９の復号ユニットの構成例を示した図。
【図５２】図５１の復号ユニットの動作を説明するためのフローチャート。
【図５３】本発明に係る情報記録装置および情報再生装置を用いた情報流通システムの構成例を示した図。
【図５４】本発明の第２の実施形態に係る復号ユニットＡの構成例を示した図。
【図５５】復号ユニットＡに入力するライセンス情報の一例を示した図。
【図５６】復号ユニットＡから出力する更新情報の一例を示した図。
【図５７】復号ユニットＡの処理動作を説明するためのフローチャート。
【図５８】復号ユニットＡの鍵保持部、鍵生成部における鍵生成処理の概略手順を説明するためのフローチャート。
【図５９】復号ユニットＢの構成例を示した図。
【図６０】復号ユニットＢに入力するライセンス情報の一例を示した図。
【図６１】復号ユニットＢの処理動作を説明するためのフローチャート。
【図６２】復号ユニットＢから出力する更新情報の一例を示した図。
【図６３】復号ユニットＣの構成例を示した図。
【図６４】復号ユニットＣから出力する更新情報の一例を示した図。
【図６５】復号ユニットＤの構成例を示した図。
【図６６】復号ユニットＤに入力するライセンス情報の一例を示した図。
【図６７】復号ユニットＤの処理動作を説明するためのフローチャート。
【図６８】復号ユニットＤの処理動作を説明するためのフローチャート。
【図６９】復号ユニットＤから出力する更新情報の一例を示した図。
【図７０】復号ユニットＤ’の構成例を示した図。

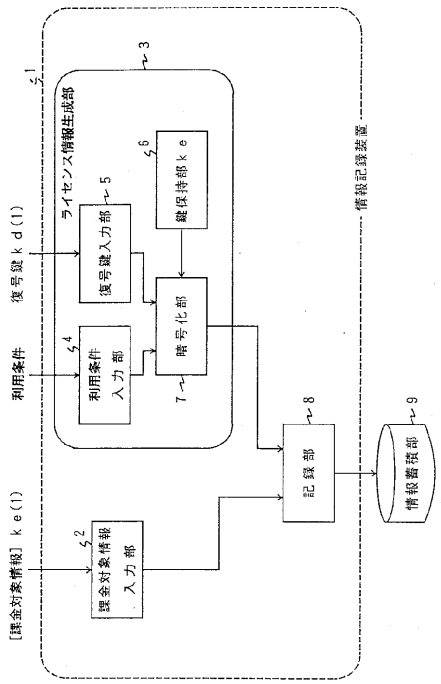
【図７１】復号ユニットＡに対応するライセンス情報更新装置の構成例を示した図。
【図７２】図７１のライセンス情報更新装置の処理動作を説明するためのフローチャート。
【図７３】復号ユニットＢに対応するライセンス情報更新装置の構成例を示した図。
【図７４】図７３のライセンス情報更新装置の処理動作を説明するためのフローチャート。
【図７５】第３の実施形態に係る情報流通システムの構成例を示した図。
【図７６】第３の実施形態に係る情報流通システムの他の構成例を示した図。
【図７７】復号判定カードを装着した情報再生装置の要部の構成例を示した図。
【図７８】図７５の情報流通システムで用いられる図７７の情報再生装置の処理動作を説明するためのフローチャート。
【図７９】復号判定カードの要部の構成例を示した図。
【図８０】図７９の復号判定カードの処理動作を説明するためのフローチャート。
【図８１】図７９の復号判定カードの時刻転送部の構成例を示した図。
【図８２】図８１の時刻転送部の認証部の構成例を示した図。
【図８３】図８２の認証部の処理動作を説明するためのフローチャート。
【図８４】図７９の復号判定カードのコンテンツキー転送部の構成例を示した図。
【図８５】図８４のコンテンツキー転送部の認証部の構成例を示した図。
【図８６】図８５の認証部の処理動作を説明するためのフローチャート。
【図８７】図７７の時計の構成例を示した図。
【図８８】図８７の時計の認証部の構成例を示した図。
【図８９】図８８の認証部の処理動作を説明するためのフローチャート。
【図９０】図７９の復号判定部の構成例を示した図。
【図９１】図９０の復号判定部の処理動作を説明するためのフローチャート。
【図９２】図７７の情報再生部の構成例を示した図。
【図９３】図９２の情報再生部の処理動作を説明するためのフローチャート。
【図９４】図９２の情報再生部の認証部の構成例を示した図。
【図９５】図９４の認証部の処理動作を説明するためのフローチャート。
【図９６】図７７の情報再生部の他の構成例を示した図。
【図９７】ライセンス更新装置の構成例を示した図。
【図９８】ライセンス更新装置の処理動作を説明するためのフローチャート。
【図９９】ライセンス更新装置の更新ＩＦとのインターフェースを司る復号判定カードの要部の構成例を示した図。
【図１００】ライセンス更新時の復号判定カードの処理動作を説明するためのフローチャート。
【図１０１】ライセンスサーバの構成例を示した図。
【図１０２】ライセンスサーバの処理動作を説明するためのフローチャート。
【図１０３】電子決済を利用してライセンスを更新する場合のユーザ端末、ライセンスサーバ、電子決済装置からなるシステム構成の一例を示した図。
【図１０４】図１０３のシステム構成におけるライセンス更新装置の構成例を示した図。
【図１０５】図１０３のシステム構成におけるライセンスサーバの構成例を示した図。
【図１０６】図１０３のシステム構成においてライセンス更新を行う場合のシステム全体の処理動作を説明するためのフローチャート。
【図１０７】本発明の第４の実施形態に係る情報再生システムの全体の構成例を示した図。
【図１０８】図１０７のライセンス判定ユニットの構成例を示した図。
【図１０９】図１０７の情報再生装置の処理動作を説明するためのフローチャート。
【図１１０】図１０７の情報再生装置の処理動作を説明するためのフローチャート。
【図１１１】図１０７の情報再生装置において、ライセンス情報をライセンスデータベースへ格納するまでの処理動作を説明するためのフローチャート。

【図１１２】図１０７の情報生成装置において、ライセンス情報の復号鍵の生成処理動作について説明するためのフローチャート。
【図１１３】コンテンツ情報の構成例を示した図。
【図１１４】ライセンス情報の構成例を示した図。
【図１１５】ライセンス情報データベースにおけるライセンス情報の記憶例を示した図。
【図１１６】ライセンス更新情報の構成例を示した図。
【図１１７】ライセンス情報データベースにおけるライセンス情報の他の記憶例を示した図。
【図１１８】図１０７に示した情報再生装置の他の構成例を示した図。
【図１１９】図１０７のライセンス判定ユニットの他の構成例を示した図。
【図１２０】図１１８の情報再生装置において、受信した放送波から暗号化ライセンス情報と復号鍵のシード情報を分離して復号鍵を生成するまでの動作について説明するためのフローチャート。
【図１２１】放送波のデータ構造の一例を示した図。
【図１２２】本発明の第５の実施形態に係る情報流通システムの構成例を示した図。
【図１２３】レンタル用のディスクに記録されているデータの一例を示した図。
【図１２４】センタに設けられたコンテンツデータベースにおけるディスクキーの記憶例w示した図。
【図１２５】図１２２に示した情報流通システムにおけるディスクキーの配送方式を概略的に示した図。
【図１２６】ライセンス作成装置の構成例を示した図。
【図１２７】ライセンス注入装置の構成例を示した図。
【図１２８】カードの構成例を示した図。
【図１２９】カードアダプタの構成例を示した図。
【図１３０】プレーヤの構成例を示した図。
【図１３１】ライセンス作成装置におけるディスク情報作成処理動作を説明するためのフローチャート。
【図１３２】ライセンス注入装置のライセンスデータベースにおけるディスク情報の記憶例を示した図。
【図１３３】図１２２の情報流通システムにおけるディスクキーの配信手順の概略をディスクレンタルサービスへの加入時、ディスクのレンタル時、コンテンツ再生時の順に示したシーケンス図。
【図１３４】図１３３に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１３５】図１３３に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１３６】図１３３に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１３７】図１３３に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１３８】図１３３に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１３９】図１３３に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１４０】図１３３に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１４１】図１２２の情報流通システムにおけるディスクキーの他の配信手順の概略をディスクレンタルサービスへの加入時・ディスクのレンタル時、コンテンツ再生時の順に示したシーケンス図。
【図１４２】図１４１に示したディスクキーの配信手順をより詳細に示したフローチャー

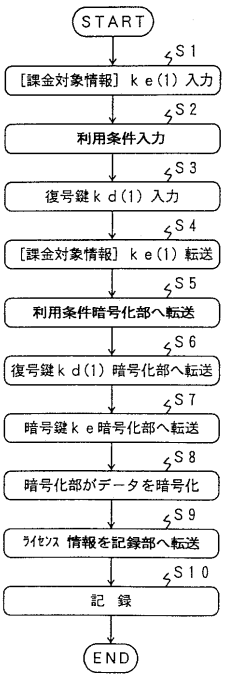
ト。
【図１４３】図１４１に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１４４】図１４１に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１４５】図１４１に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１４６】図１４１に示したディスクキーの配信手順をより詳細に示したフローチャート。
【図１４７】暗号パラメータ更新処理動作を説明するためのフローチャート。
【図１４８】暗号パラメータ更新処理動作を説明するためのフローチャート。
【図１４９】暗号パラメータ更新処理動作を説明するためのフローチャート。
【図１５０】本発明の第６の実施形態に係る情報流通システムの構成例を示した図。
【図１５１】レンタルサービス提供のために、ディスク、会員カード、再生装置のそれぞれにおいて用いられる情報データについて説明するための図。
【図１５２】再生装置の構成例を示した図。
【図１５３】図１５２の再生装置の処理動作の概略を説明するためのフローチャート。
【図１５４】ポイント加算処理動作を説明するためのフローチャート。
【図１５５】ライセンス判定処理動作を説明するためのフローチャート。
【図１５６】ポイント減算処理動作を説明するためのフローチャート。
【図１５７】コンテンツ表示処理動作を説明するためのフローチャート。
【図１５８】暗号鍵Ｋｔの更新処理動作を説明するためのフローチャート。
【図１５９】ライセンス／ポイント注入装置の構成例を示した図。
【図１６０】ライセンス／ポイント注入装置のライセンス情報発行処理動作を説明するためのフローチャート。
【図１６１】ライセンス／ポイント注入装置のポイント情報発行処理動作を説明するためのフローチャート。
【図１６２】センター装置の構成例を示した図。
【図１６３】センター装置のライセンス情報発行処理動作を説明するためのフローチャート。
【図１６４】センター装置のポイント情報発行処理動作を説明するためのフローチャート。
【図１６５】本発明の第７の実施形態に係る情報流通システムに用いられる再生装置の構成例を示した図。
【図１６６】メディア記録情報の一例を示した図。
【図１６７】図１６５の再生装置の処理動作について説明するためのフローチャート。
【図１６８】再生装置の他の構成例を示した図。
【図１６９】再生装置のさらに他の構成例（図１７０のメディア記録情報を用いた場合）を示した図。
【図１７０】メディア記録情報の他の例を示した図。
【図１７１】図１７０のメディア記録情報を用いた場合の１６９の再生装置の処理動作について説明するためのフローチャート。
【図１７２】ＷＭ情報の埋め込み位置について説明するための図。
【符号の説明】
１…情報記録装置、２…課金対象情報入力部、３…ライセンス情報生成部、４…利用条件入力部、５…復号鍵入力部、６…鍵保持部、７…暗号化部、８…記録部、９…情報蓄積部、１００…情報再生装置、１０１…情報蓄積部、１０２…読み出し部、１０３…復号ユニット、１０４…再生部、１００１…情報記録装置、１００２…ライセンス情報再生部、１００３…情報記録部、１００４…情報蓄積部、１０１１…情報記録装置、１０１２…読み出し部、１０１３…復号ユニット、１０１４…再生部、１０１５…情報蓄積部。

２００１…ライセンス情報入力部、２００２…復号部、２００３…判定部、２００４…更新情報生成部、２００５…鍵保持部、２００６…鍵生成部、２００７…時計参照部、２００８…ライセンス情報更新装置、２００９…利用条件入力部、２０１０…時計、２０２０…情報利用装置。
３００１…復号判定カード、３００２…リムーバブルメディア読取装置、３００３…リムーバブル情報蓄積メディア、３００４…情報再生部、３００５…時計。
５００１…ライセンス作成装置、５００２…コンテンツデータベース（ＤＢ）、５００３…ライセンス注入装置、５００４…カードアダプタ、５００５…プレーヤ、Ｐ…カード、Ｄ…レンタル用ディスク、７０００…情報再生装置、７００１…情報メディアドライバ、７００２…情報利用装置、７００８、８００９…ライセンス判定ユニット。
７１０１…再生装置、７１０２…会員カード、７１０３…情報記録メディア（ディスク）、７１１１…ライセンス／ポイント注入装置、７１２１…センター装置。
８１０１…メディア、８１０２…メディア読取部、８１０３…復号ユニット、８１１０…カード、８１１２…表示装置、８１２１…放送波受信部（チューナ）。

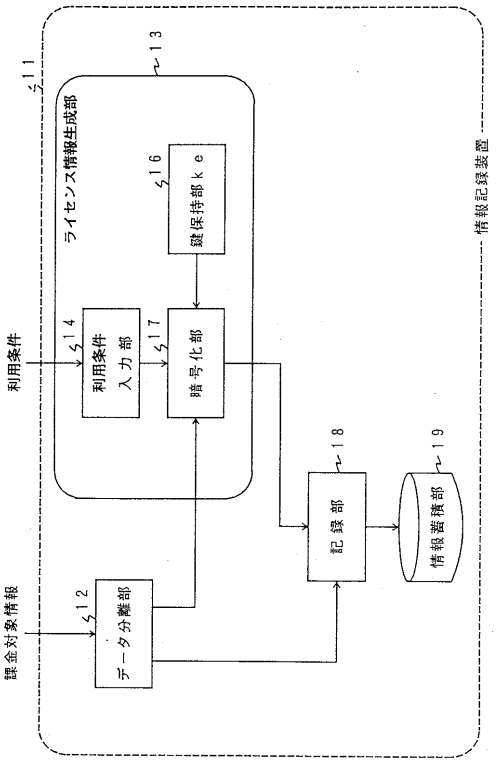
【図１】



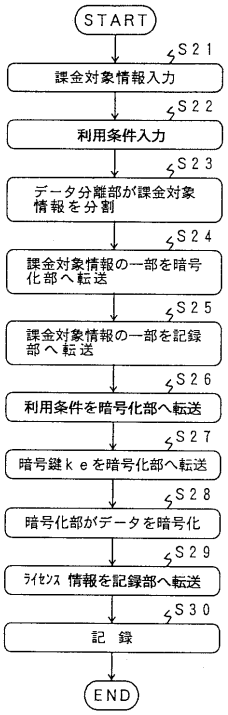
【図２】



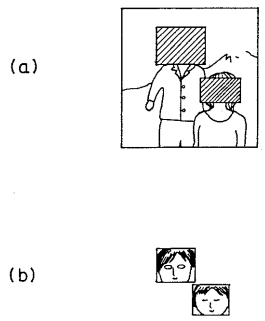
【図３】


情報記録装置
11
ライセンス情報生成部
13
鍵保持部ｋｅ
16
利用条件
利用条件入力部
14
暗号化部
17
課金対象情報
データ分離部
12
記録部
18
情報蓄積部
19

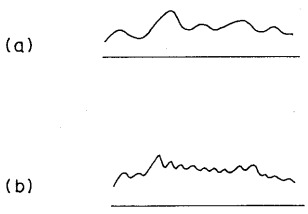
【図４】


START
S21
課金対象情報入力
S22
利用条件入力
S23
データ分離部が課金対象情報を分割
S24
課金対象情報の一部を暗号化部へ転送
S25
課金対象情報の一部を記録部へ転送
S26
利用条件を暗号化部へ転送
S27
暗号鍵ｋｅを暗号化部へ転送
S28
暗号化部がデータを暗号化
S29
ﾗｲｾﾝｽ 情報を記録部へ転送
S30
記録
END

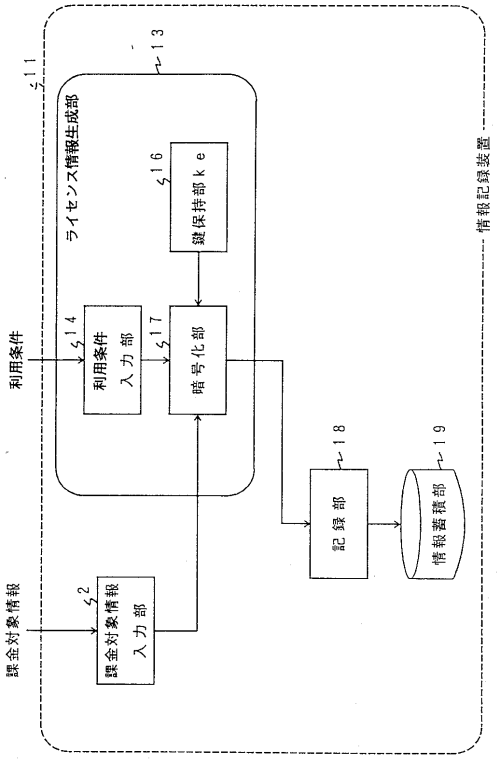
【図５】


(a)
(b)

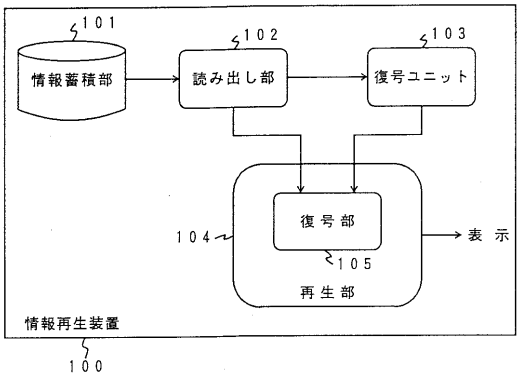
【図６】


(a)
(b)

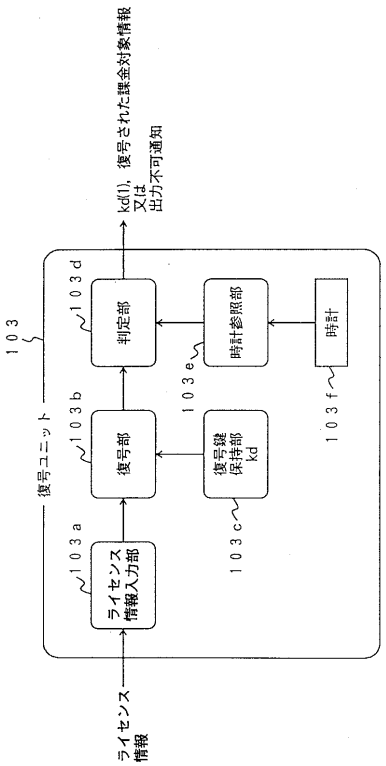
【図７】


情報記録装置
11
ライセンス情報生成部
13
鍵保持部ｋｅ
16
利用条件
利用条件入力部
14
暗号化部
17
課金対象情報
課金対象情報入力部
12
記録部
18
情報蓄積部
19

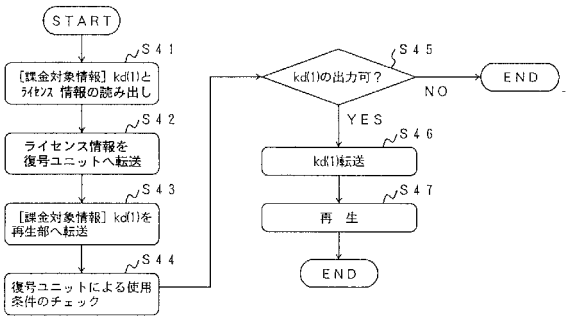
【図８】


101
情報蓄積部
102
読み出し部
103
復号ユニット
104
復号部
105
再生部
表示
情報再生装置
100

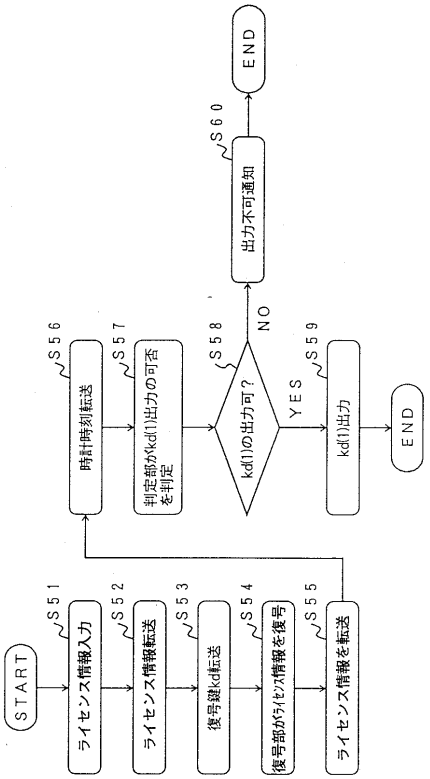
【図９】


kd(1)，復号された課金対象情報
又は
出力不可通知
103
復号ユニット
103a
ライセンス情報入力部
103b
復号部
103c
復号鍵保持部 kd
103d
判定部
103e
時計参照部
103f
時計
ライセンス情報

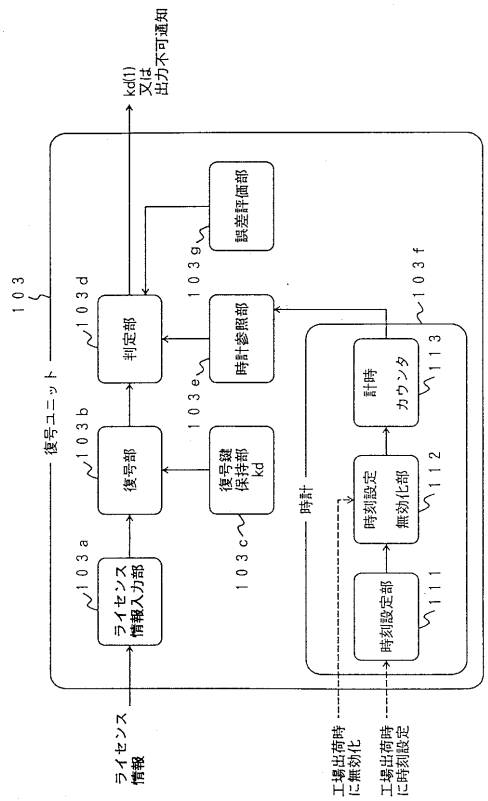
【図１０】


START
S41
[課金対象情報] kd(1)とﾗｲｾﾝｽ 情報の読み出し
S42
ライセンス情報を復号ユニットへ転送
S43
[課金対象情報] kd(1)を再生部へ転送
S44
復号ユニットによる使用条件のチェック
S45
kd(1)の出力可？
NO
END
YES
S46
kd(1)転送
S47
再 生
END

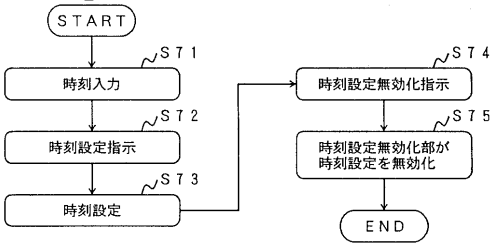
【図１１】


START
S51
ライセンス情報入力
S52
ライセンス情報転送
S53
復号鍵kd転送
S54
復号部がﾗｲｾﾝｽ情報を復号
S55
ライセンス情報を転送
S56
時計時刻転送
S57
判定部がkd(1)出力の可否を判定
S58
kd(1)の出力可？
NO
YES
S59
kd(1)出力
END
S60
出力不可通知
END

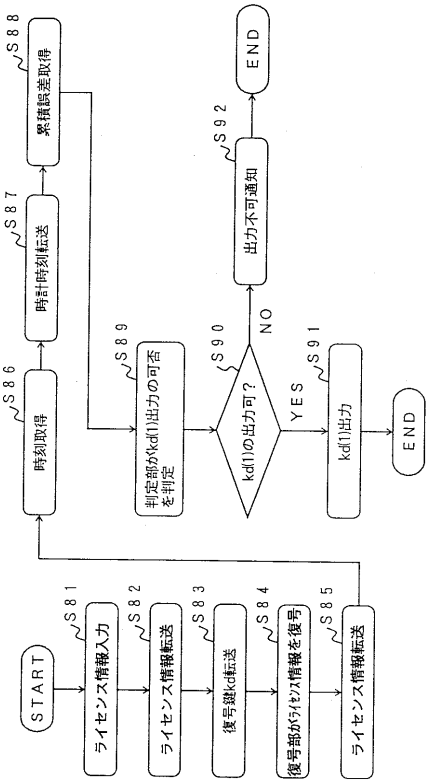
【図１２】



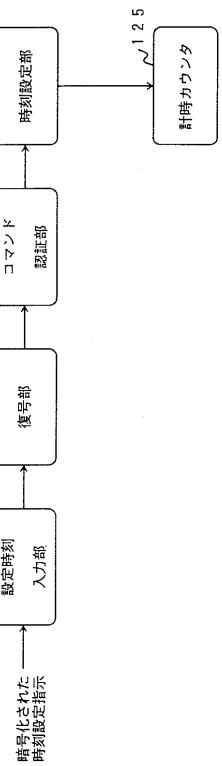
【図１３】



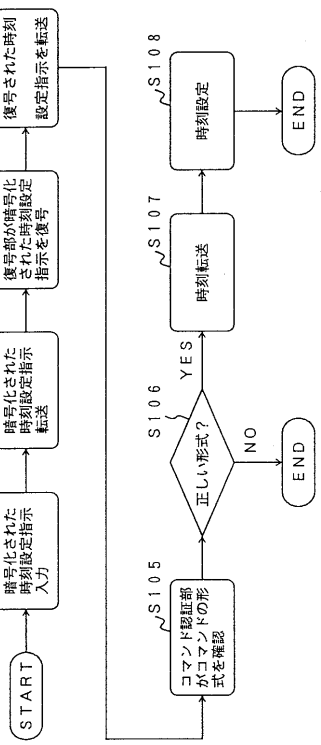
【図１４】



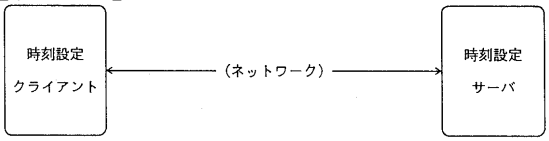
【図１５】



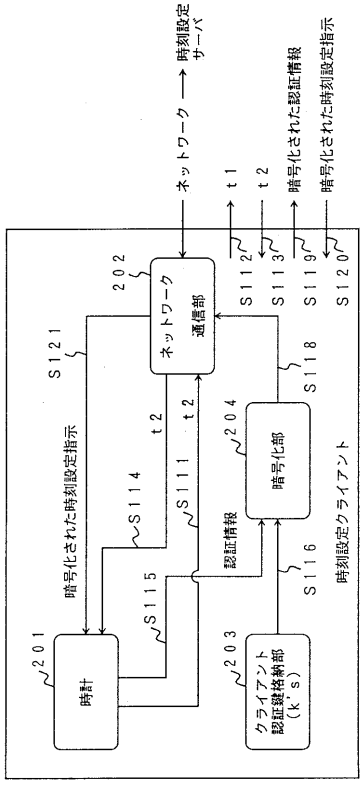
【図１６】



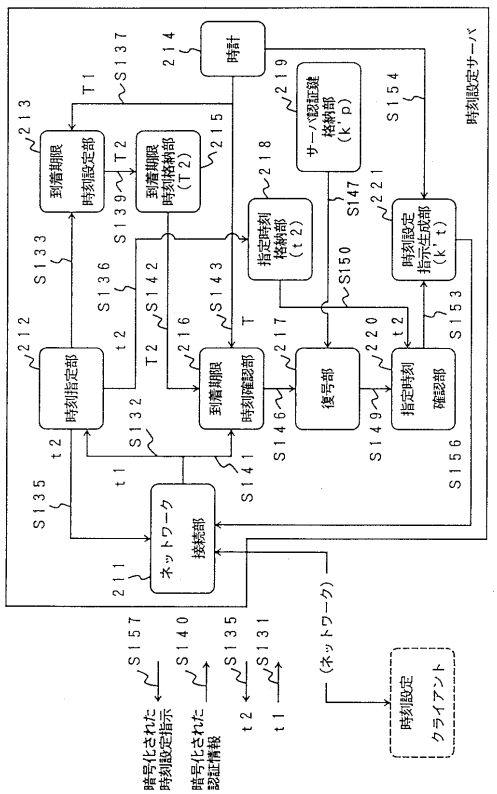
【図１７】



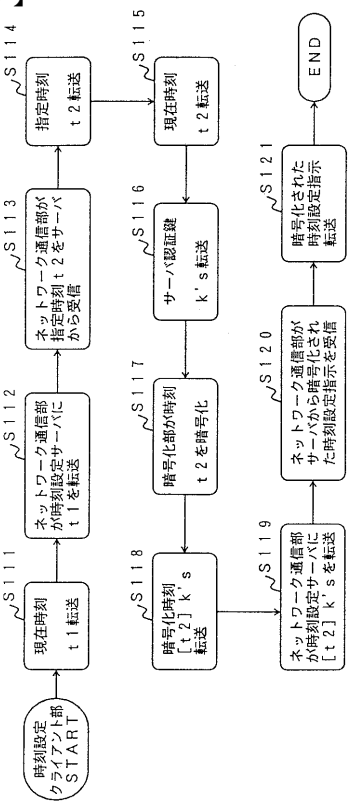
【図１８】



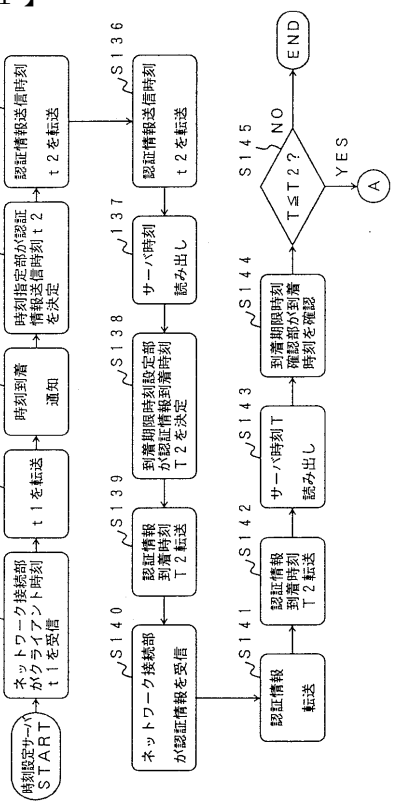
【図１９】



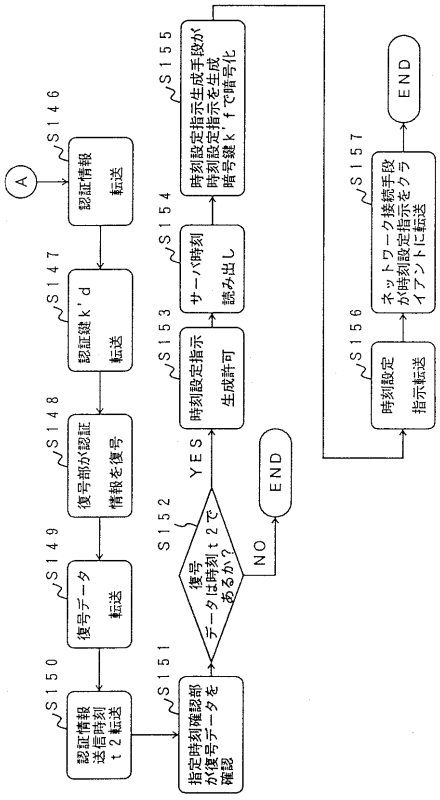
【図２０】



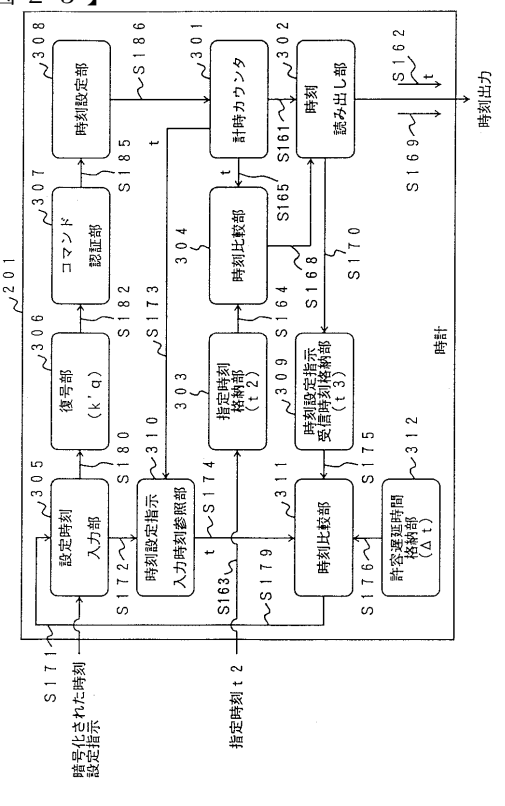
【図２１】



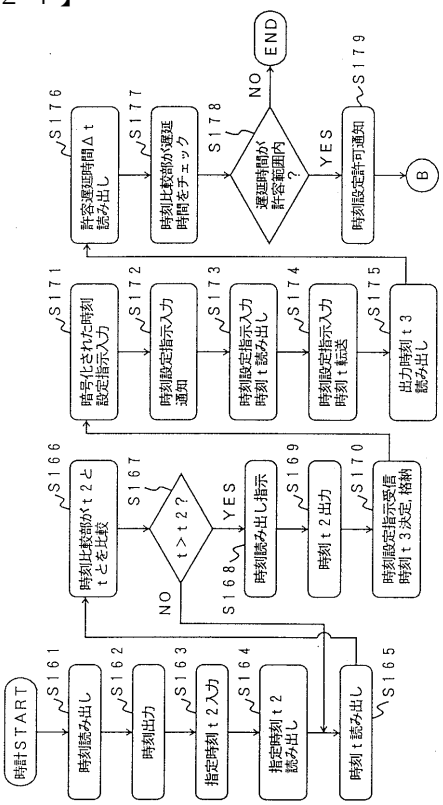
【図２２】



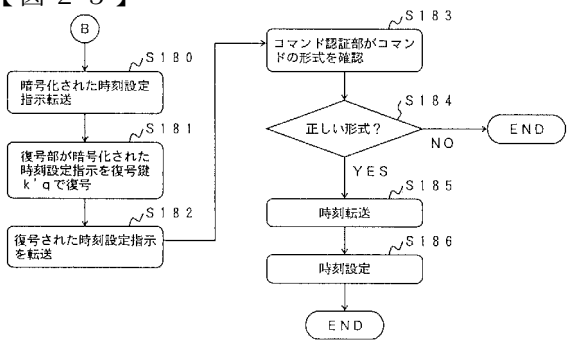
【図２３】



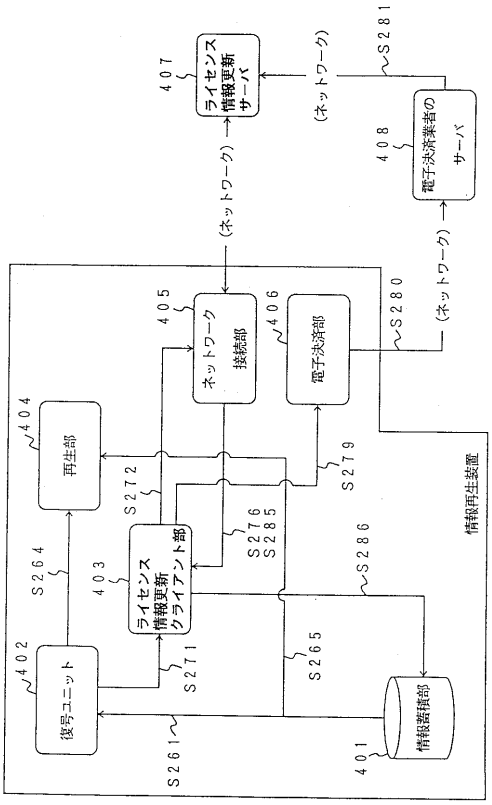
【図２４】



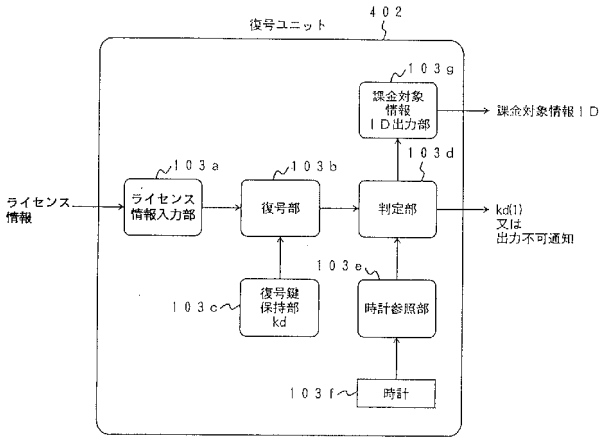
【図２５】



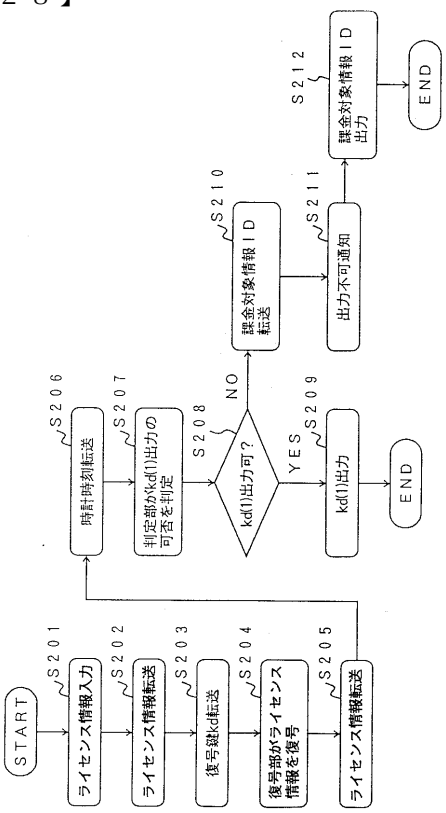
【図２６】



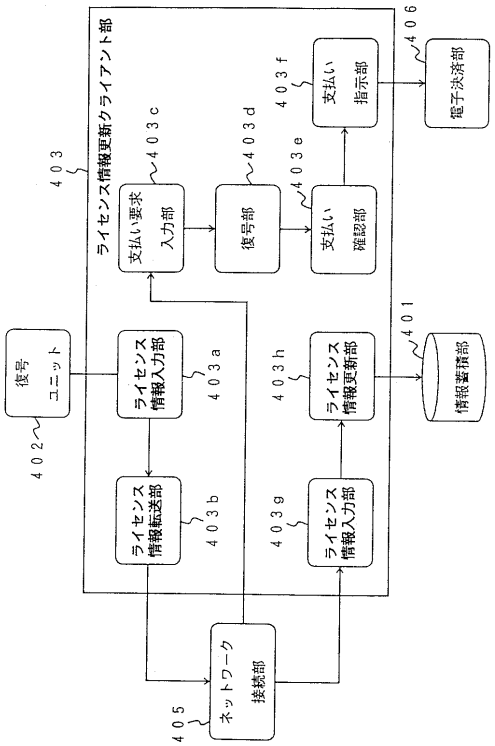
【図２７】



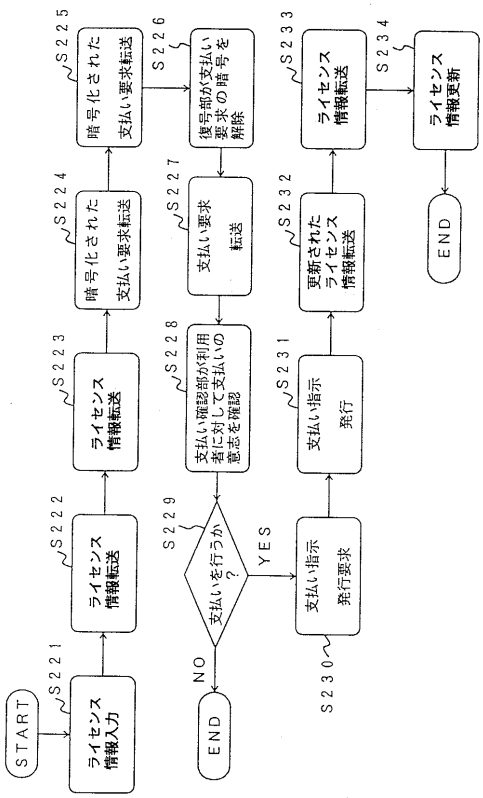
【図２８】



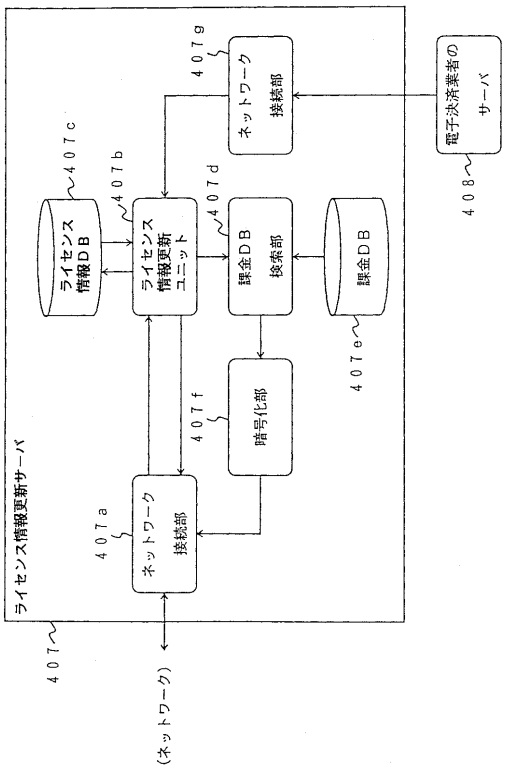
【図２９】



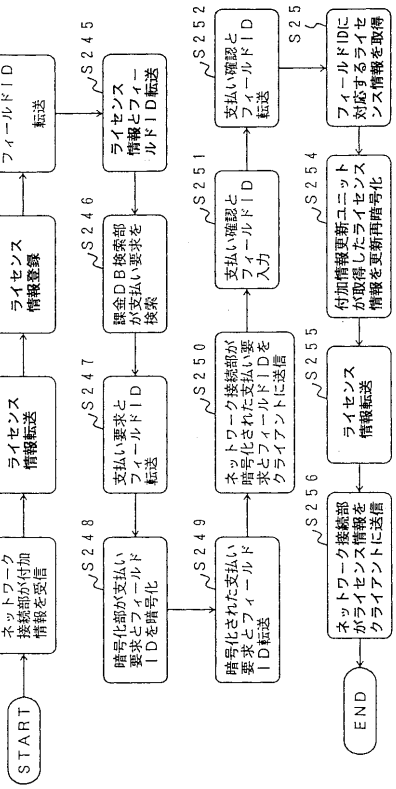
【図３０】



【図３１】



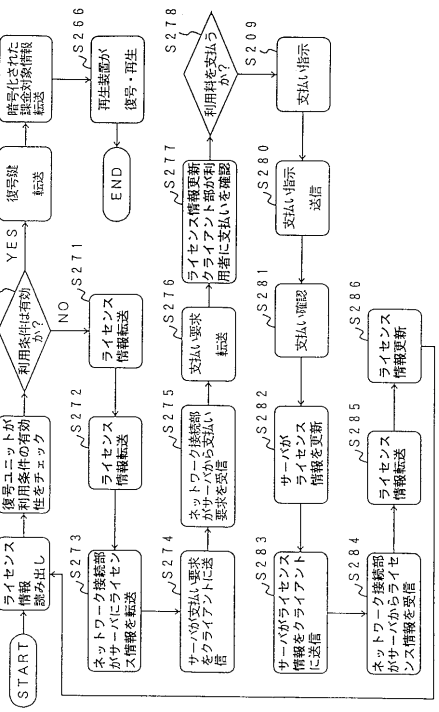
【図３２】



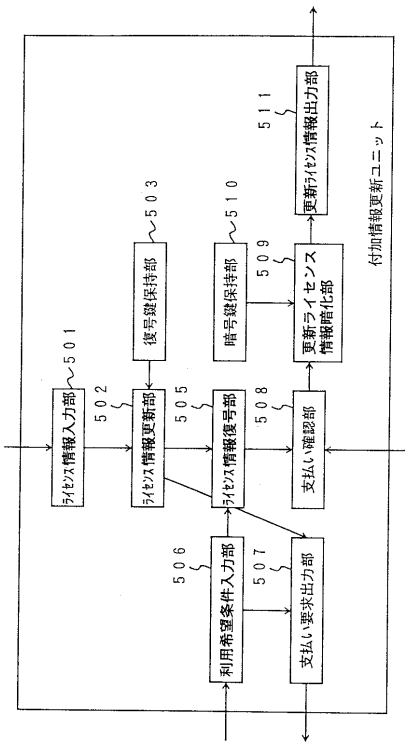
【図３３】

課金対象情報ＩＤ	１週間	２週間	１ヵ月	支配先
ＡＢＣＤ	１０円	１５円	３０円	ａｂｃ

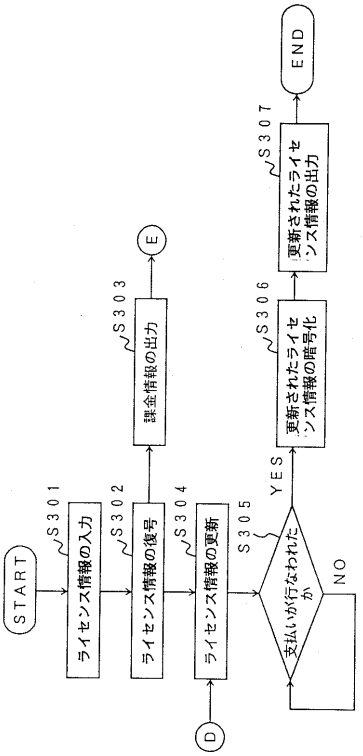
【図３４】



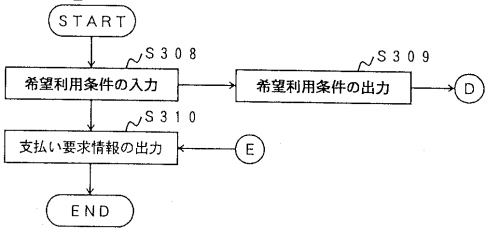
【図３５】



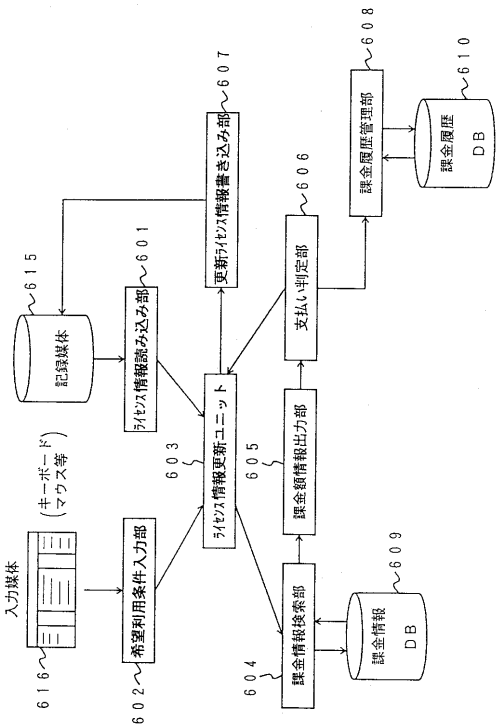
【図３６】



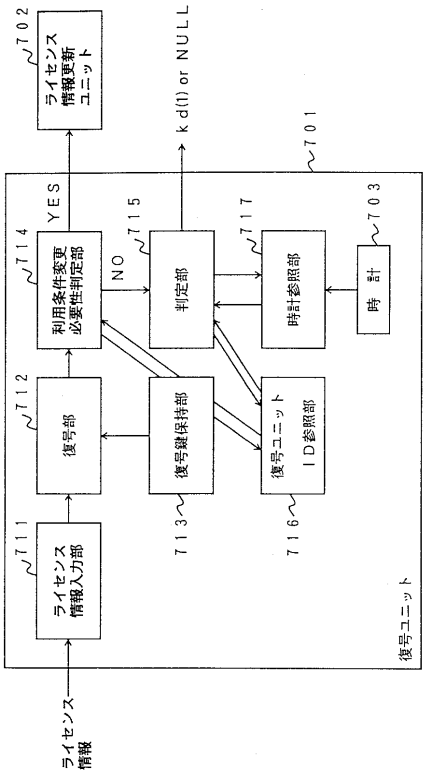
【図３７】



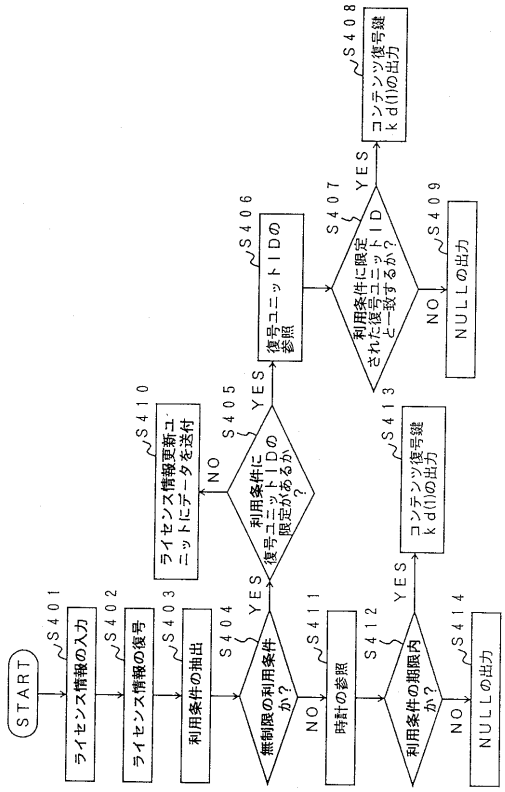
【図３８】



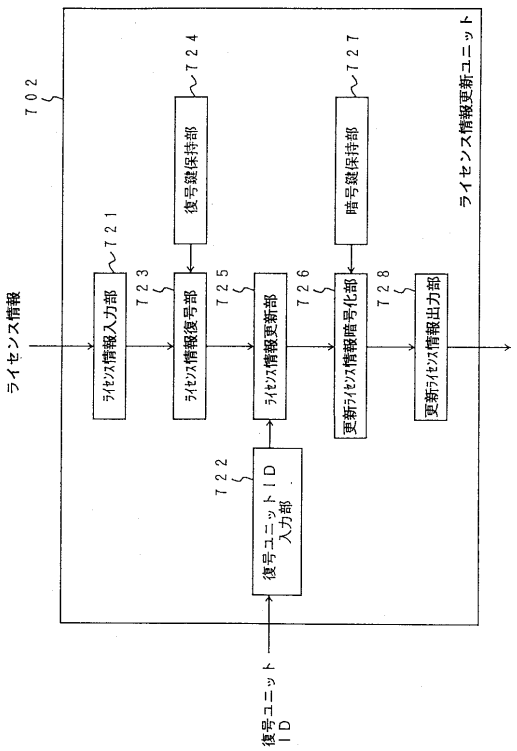
【図３９】



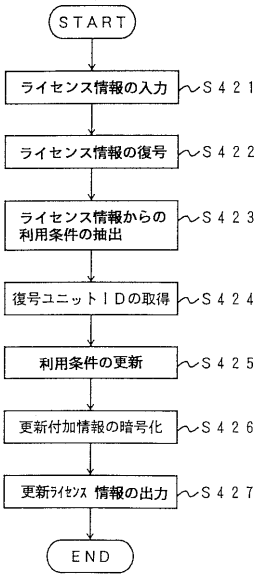
【図４０】



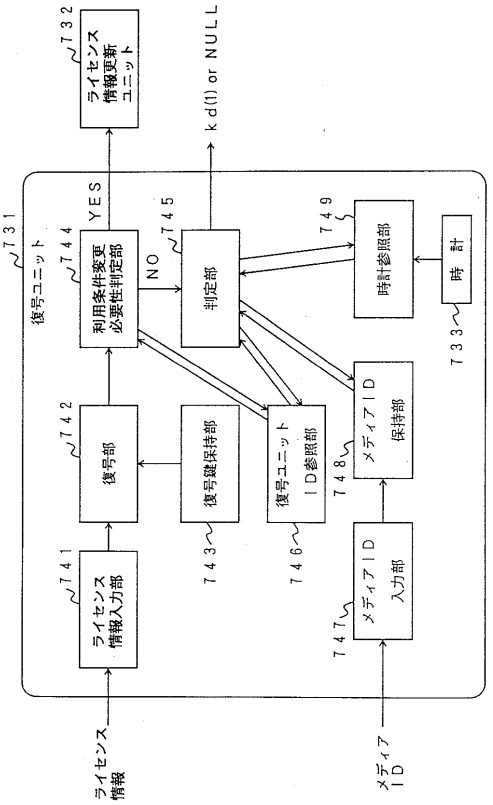
【図４１】



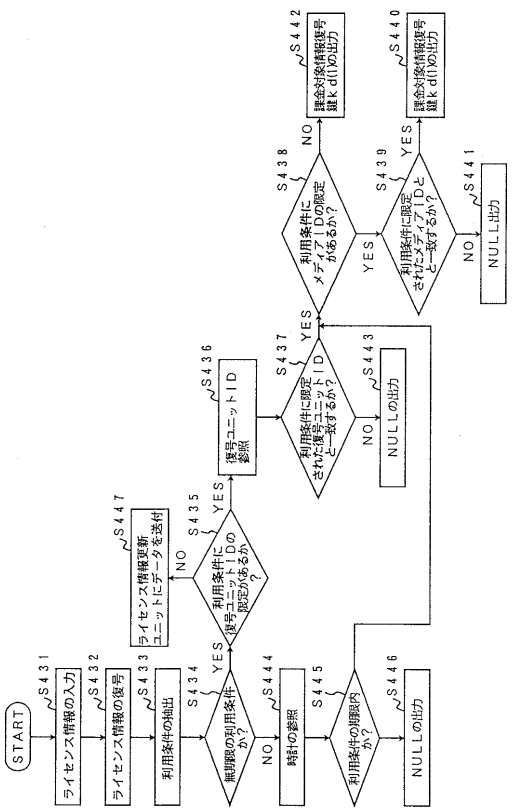
【図４２】



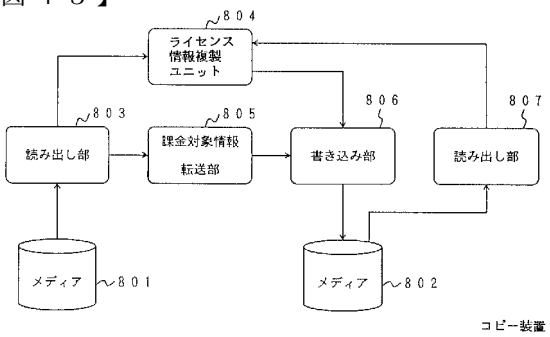
【図４３】



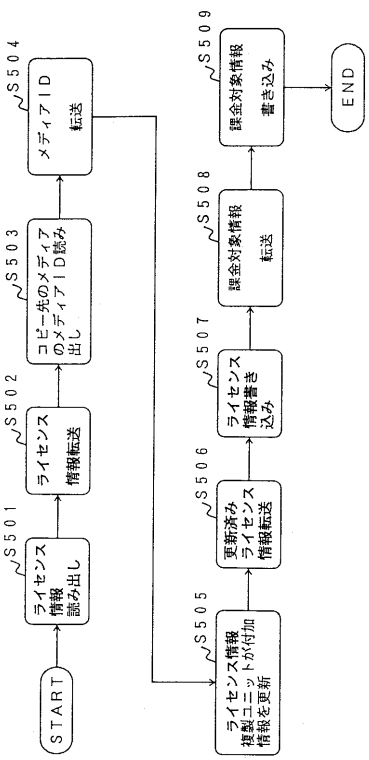
【図４４】



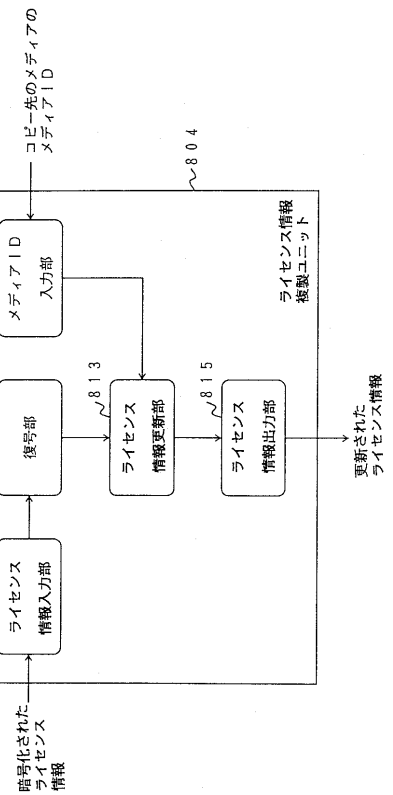
【図４５】



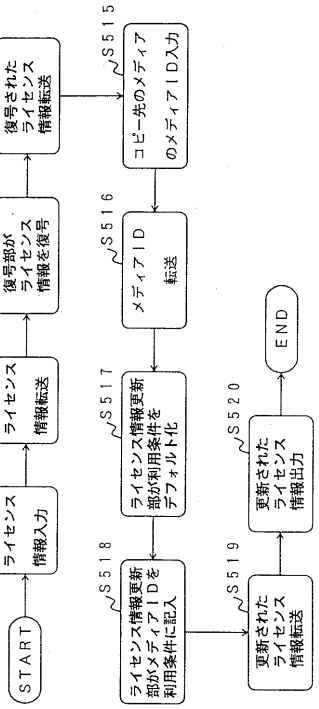
【図４６】



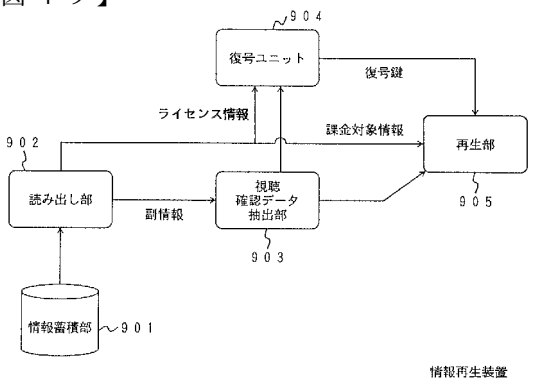
【図４７】



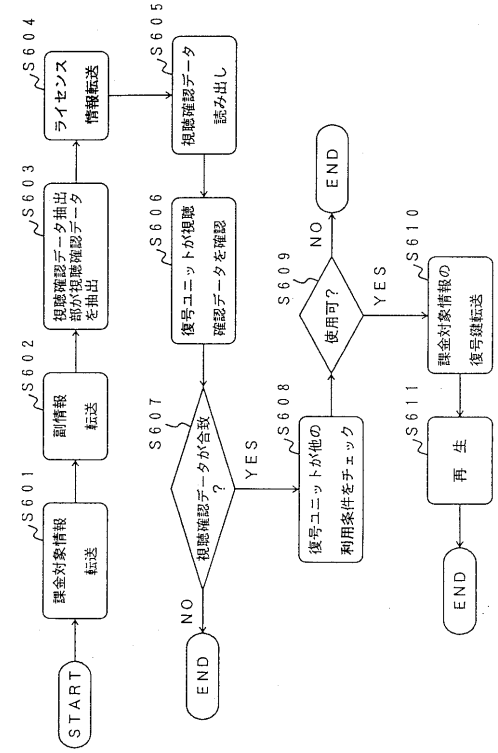
【図４８】



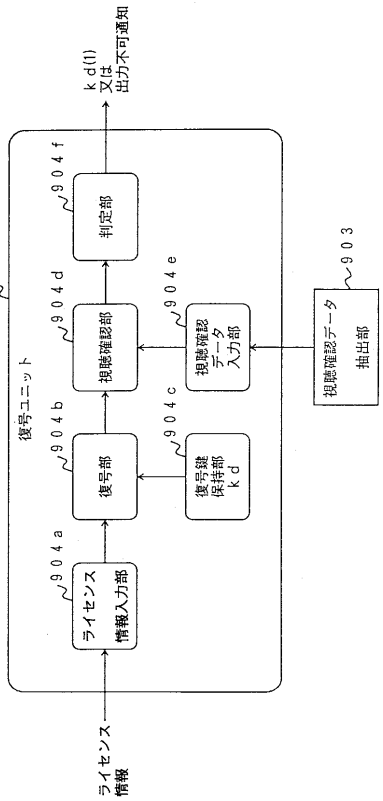
【図４９】



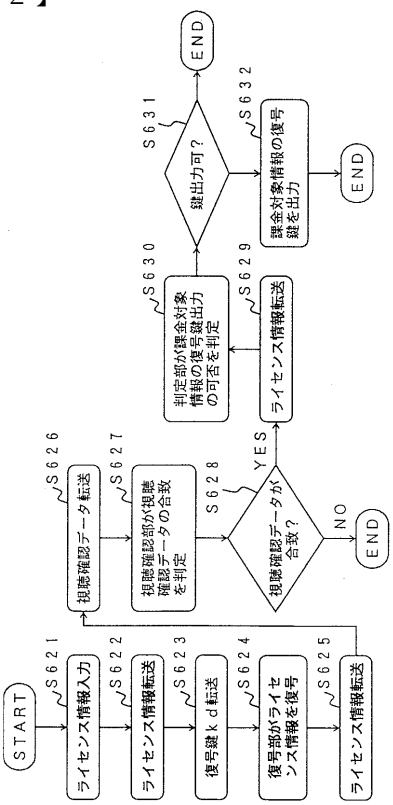
【図５０】



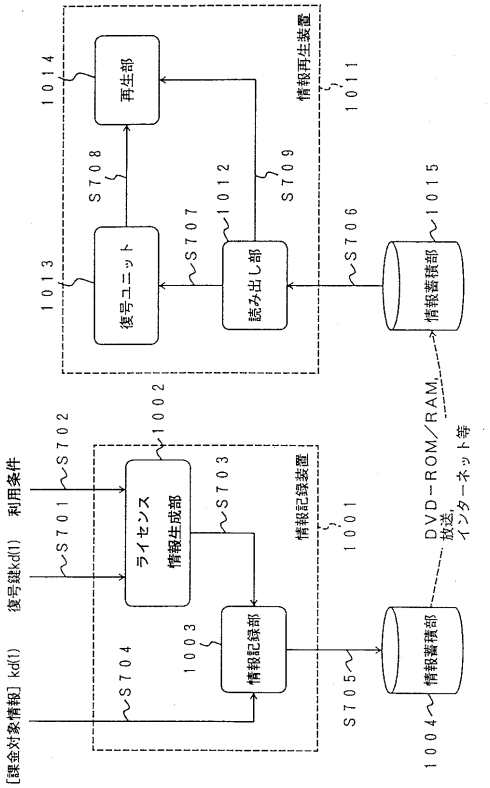
【図５１】



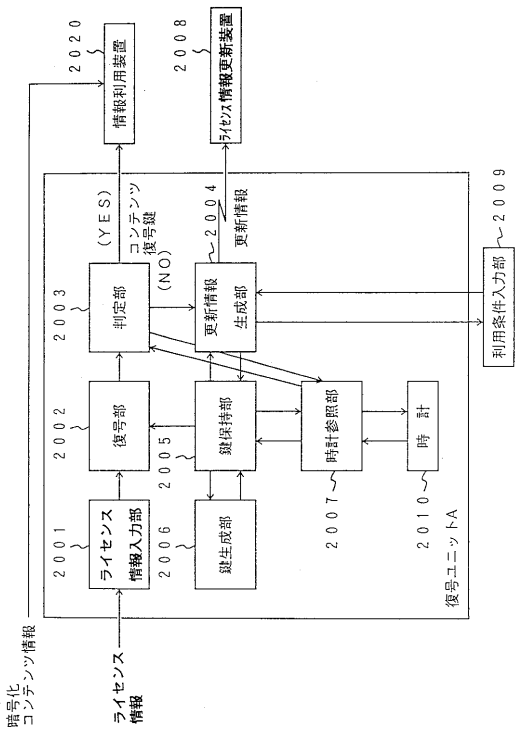
【図５２】



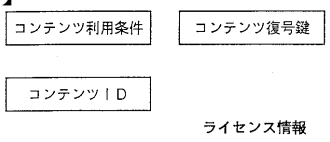
【図５３】



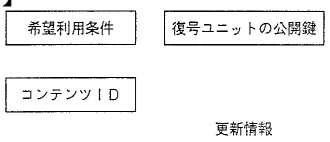
【図５４】



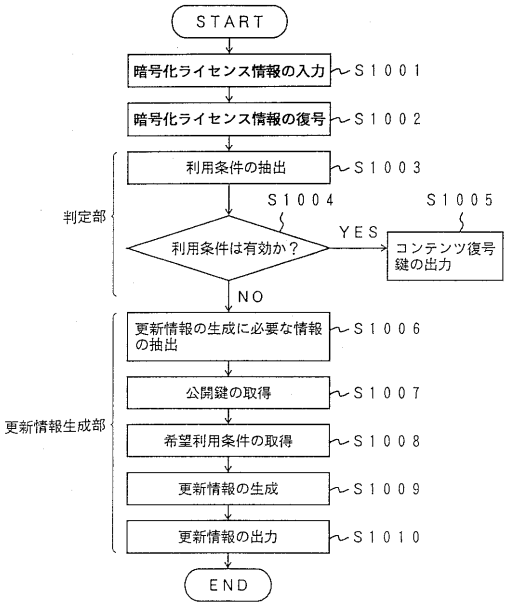
【図５５】



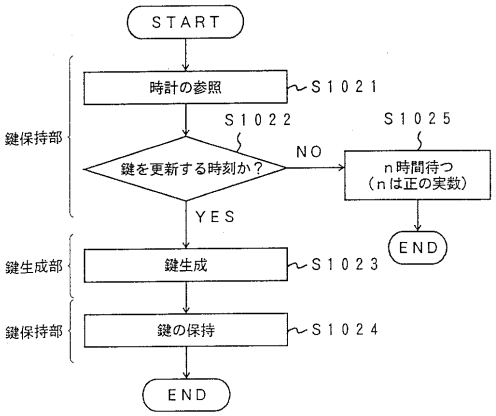
【図５６】



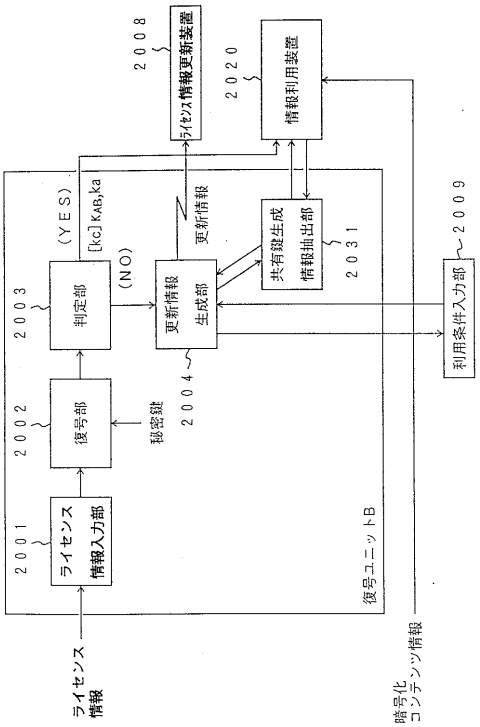
【図５７】



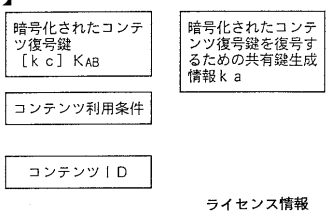
【図５８】



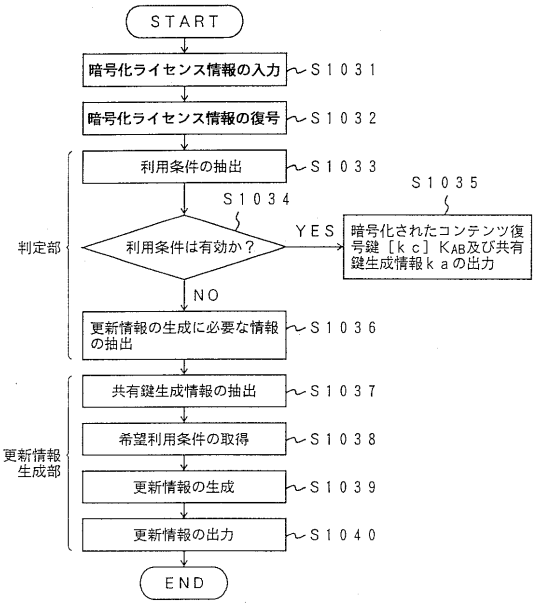
【図５９】



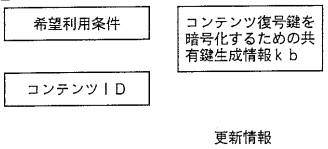
【図６０】



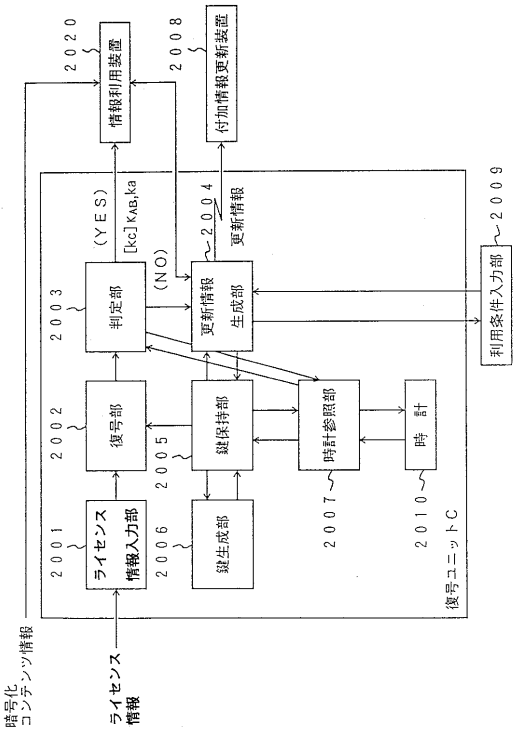
【図６１】



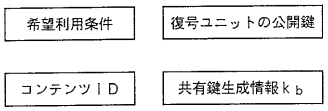
【図６２】



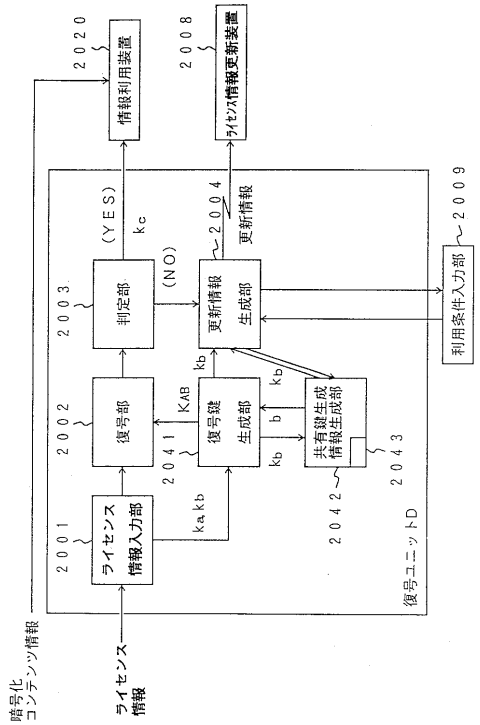
【図６３】



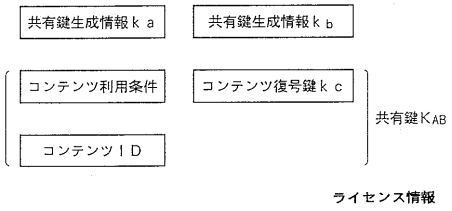
【図６４】



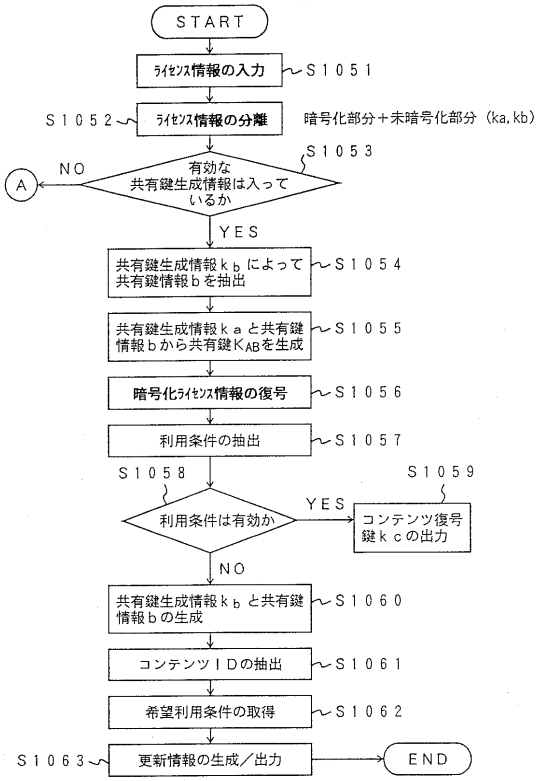
【図６５】



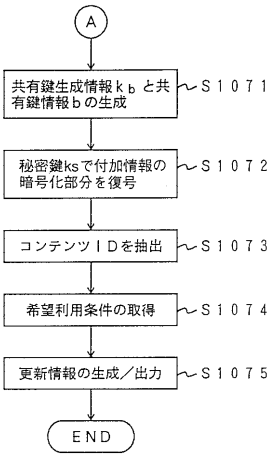
【図６６】



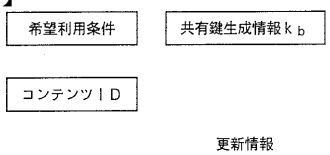
【図６７】



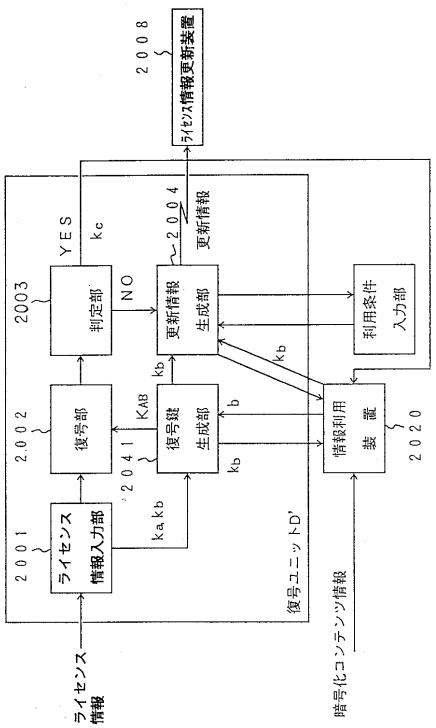
【図６８】



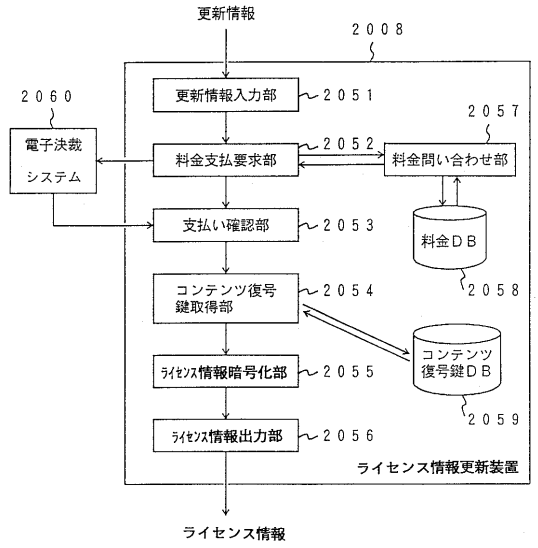
【図６９】



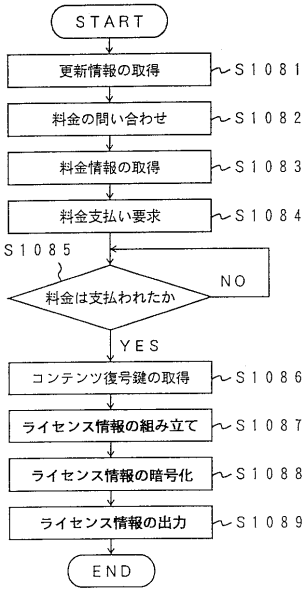
【図７０】



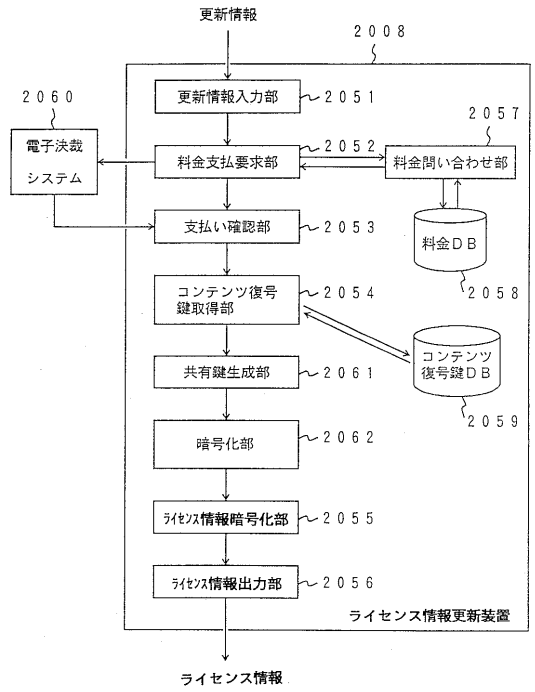
【図７１】



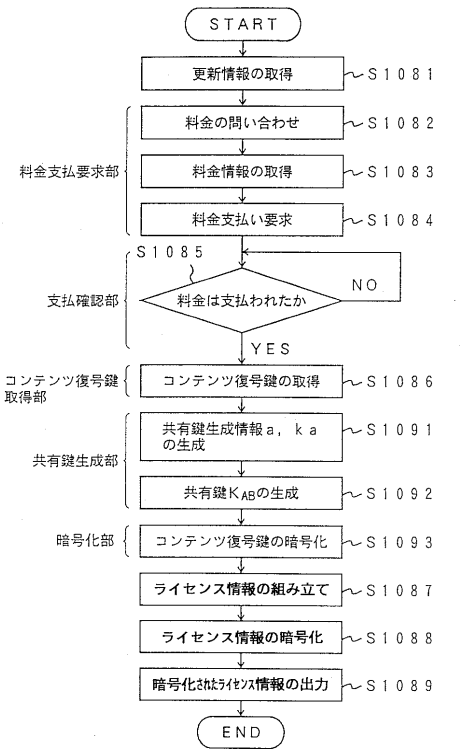
【図７２】



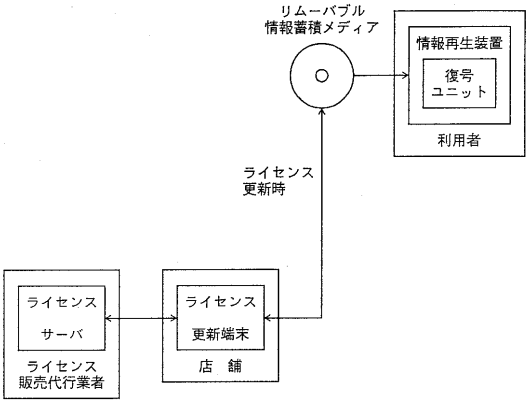
【図７３】



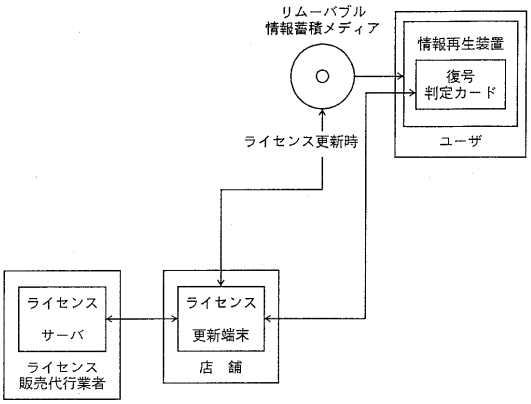
【図７４】



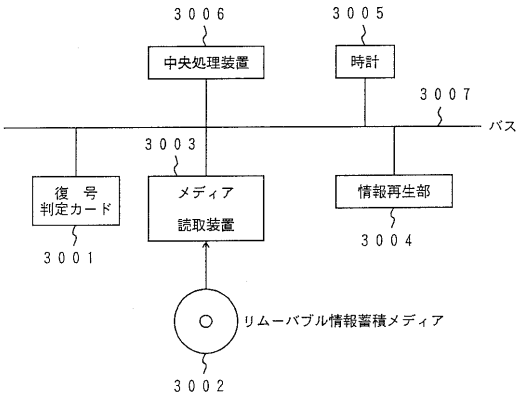
【図７５】



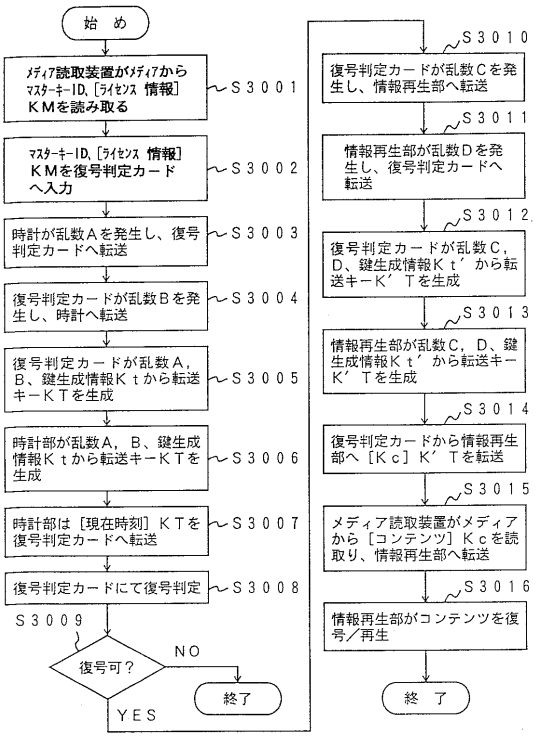
【図７６】



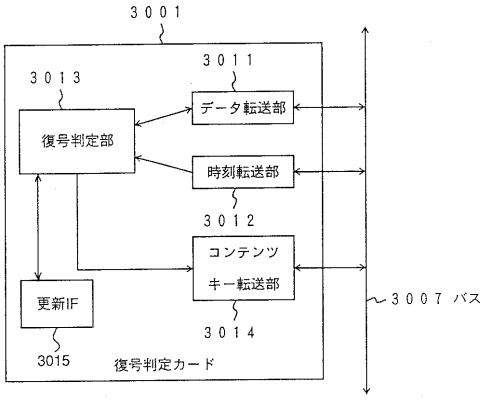
【図７７】



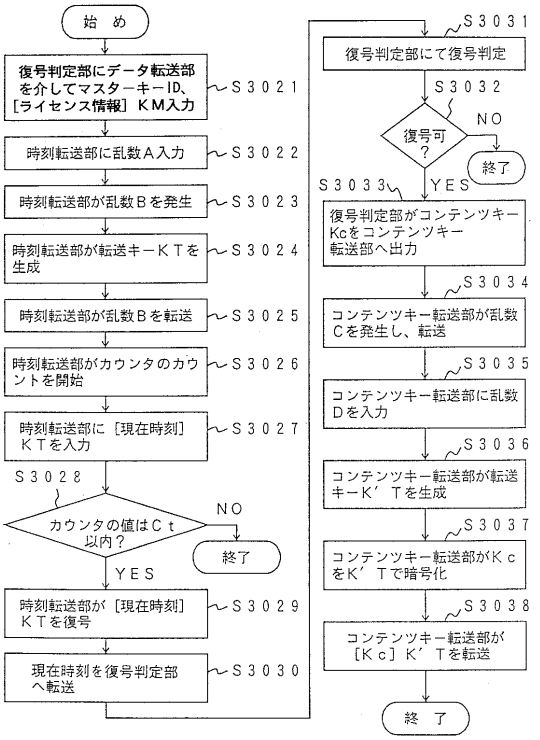
【図７８】



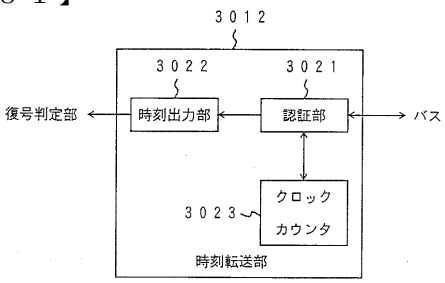
【図７９】



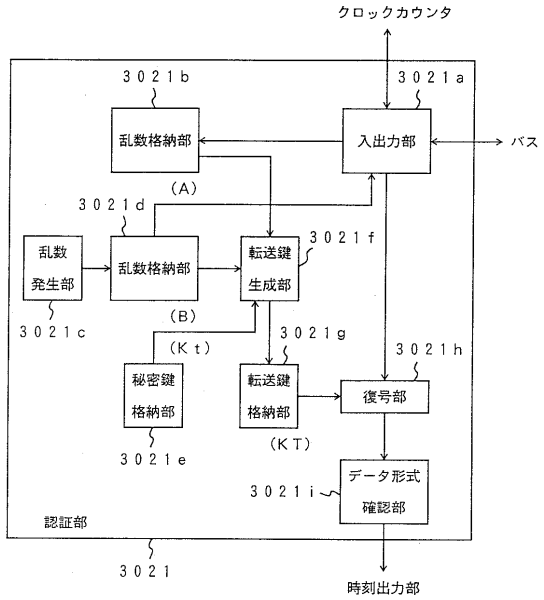
【図８０】



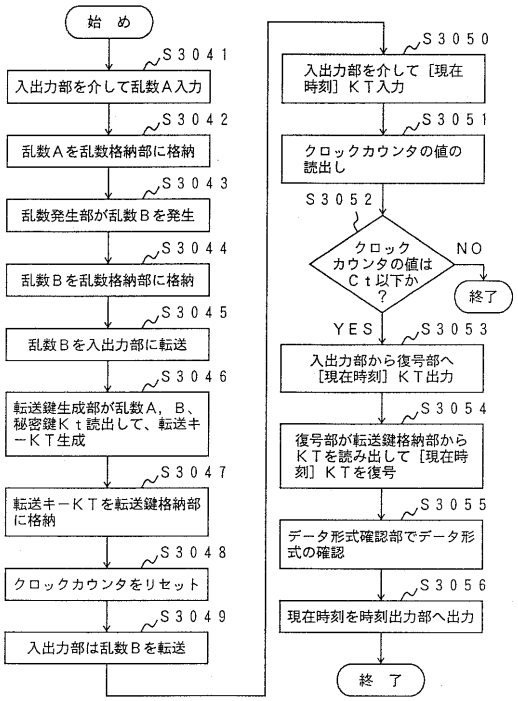
【図８１】



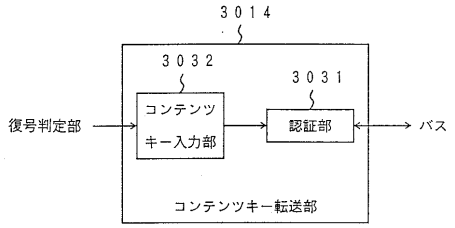
【図８２】



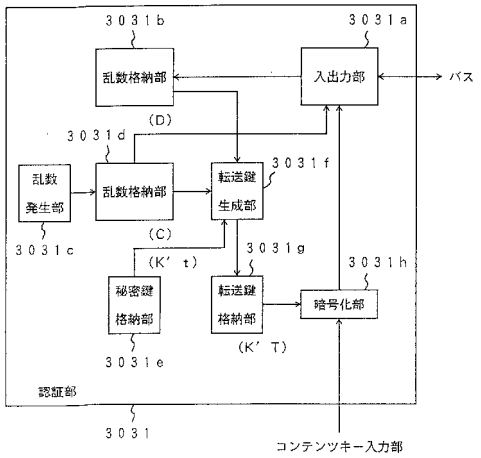
【図８３】



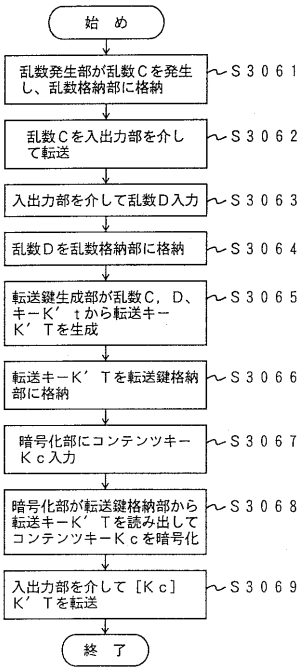
【図８４】



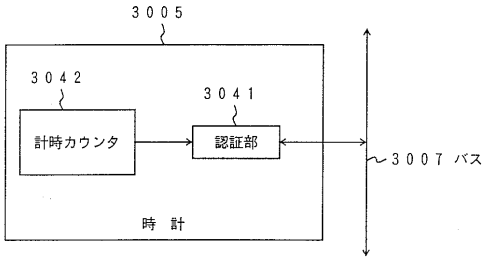
【図８５】



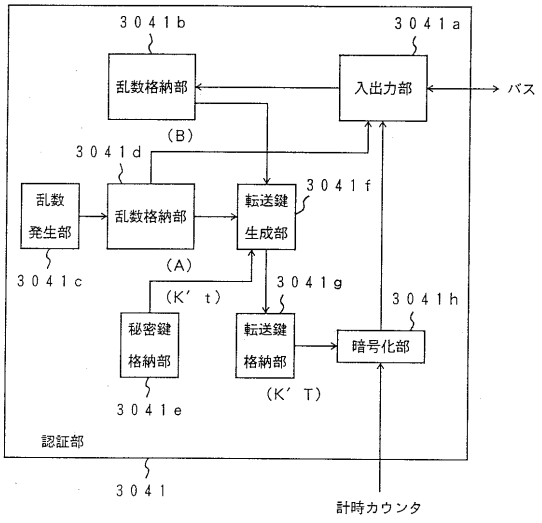
【図８６】



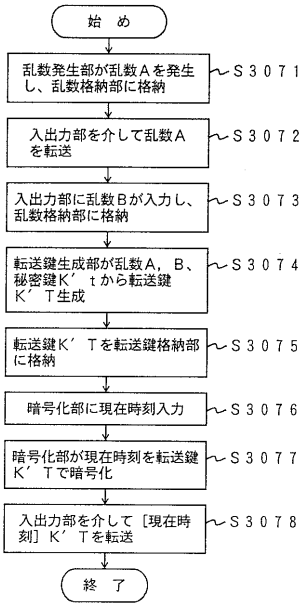
【図８７】



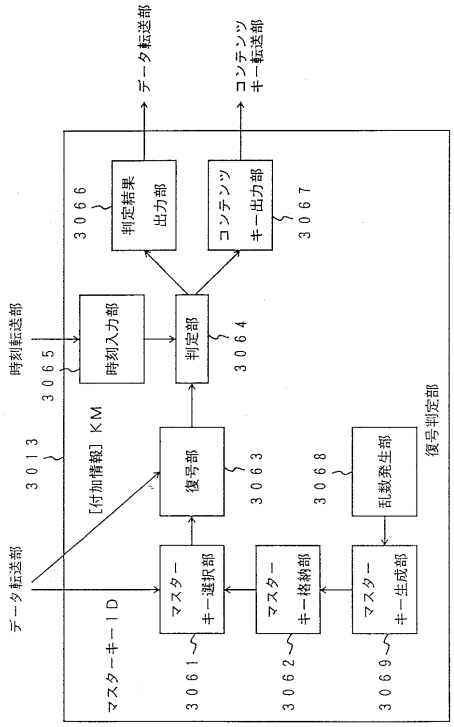
【図８８】



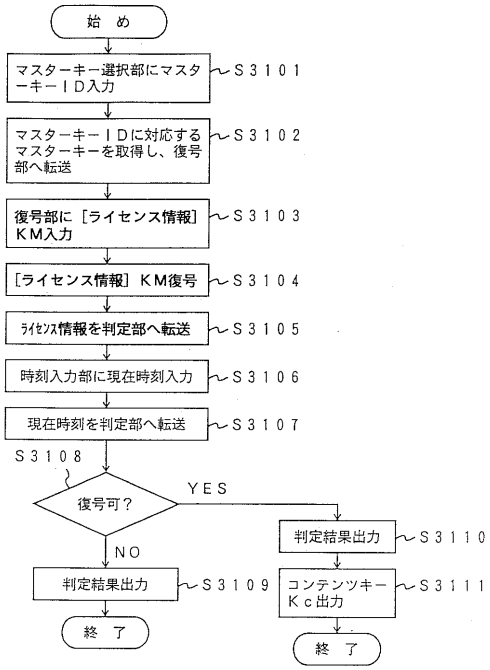
【図８９】



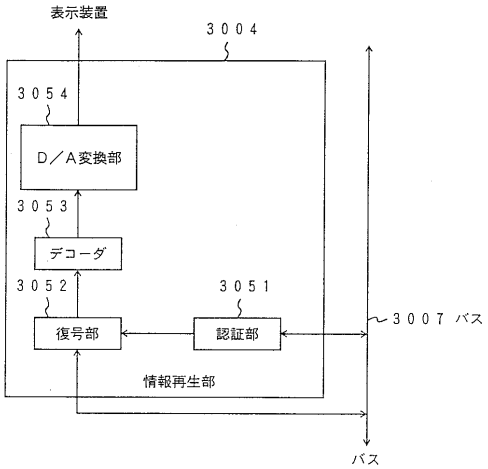
【図９０】



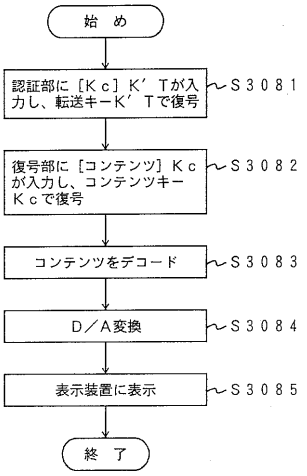
【図９１】



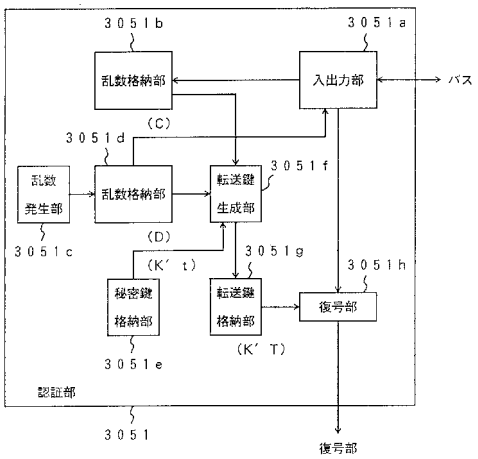
【図９２】



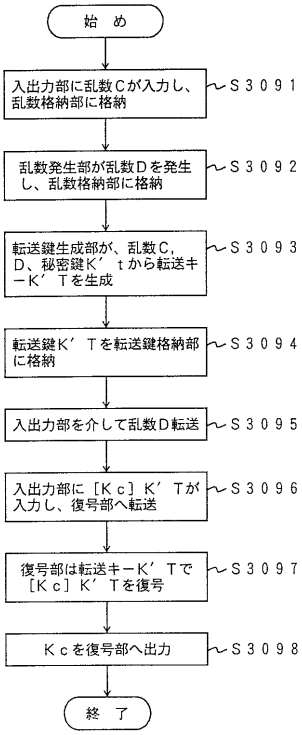
【図９３】



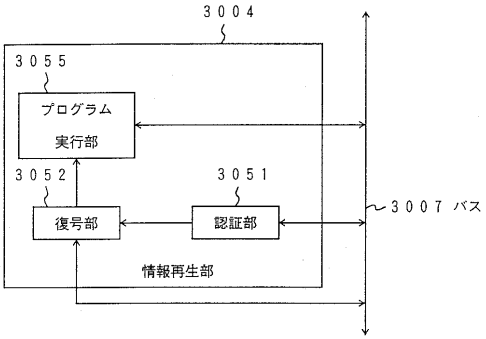
【図９４】



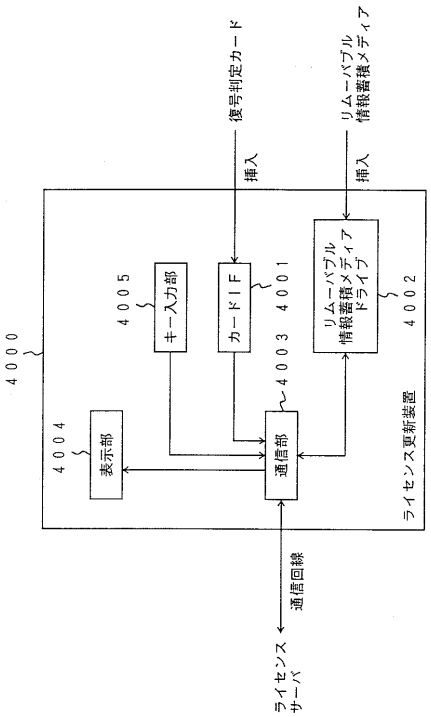
【図９５】



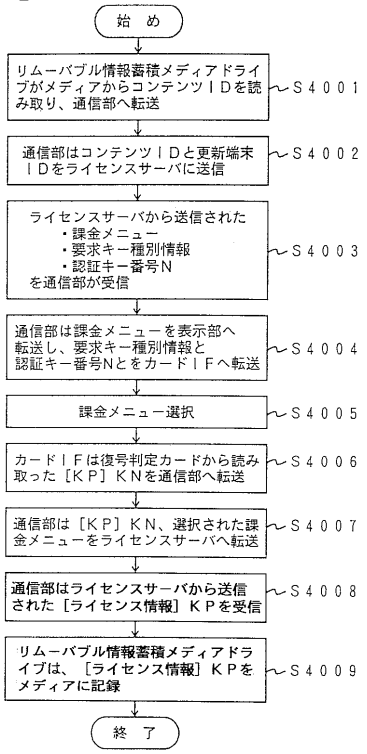
【図９６】



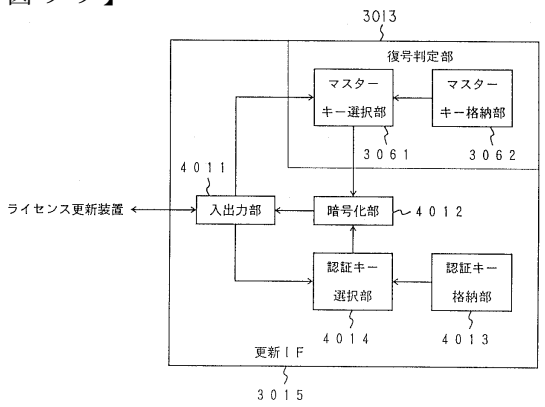
【図９７】



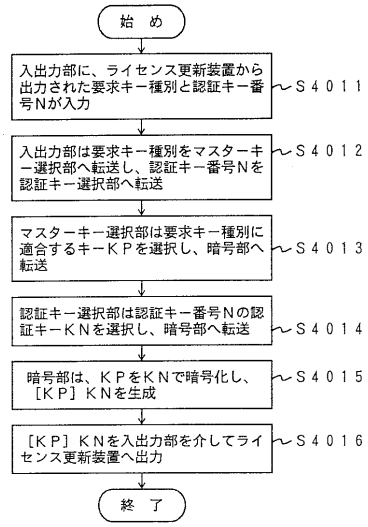
【図９８】



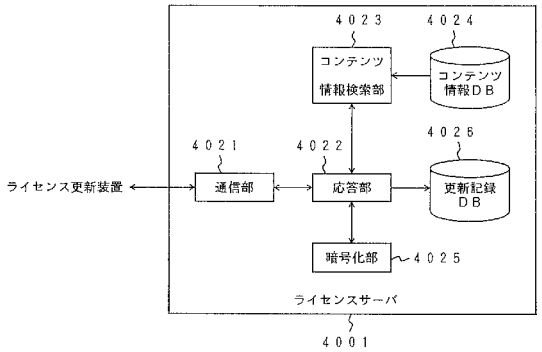
【図９９】



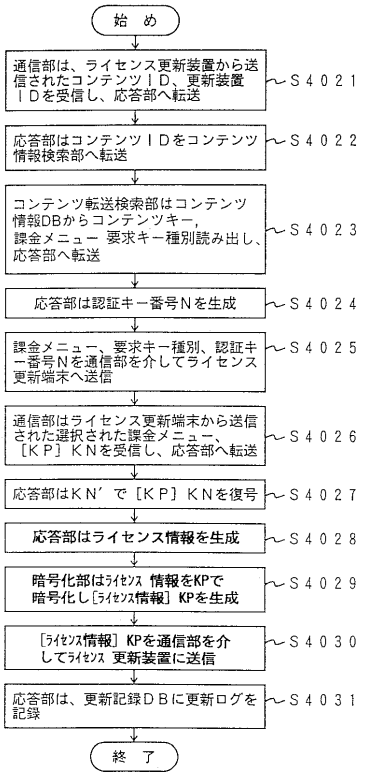
【図１００】



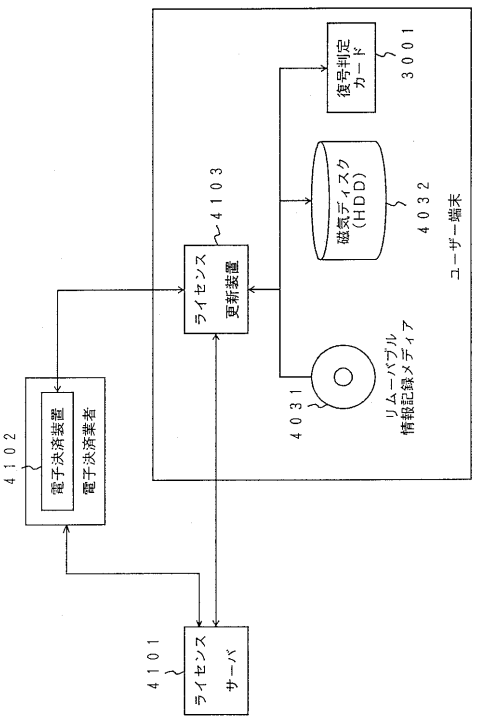
【図１０１】



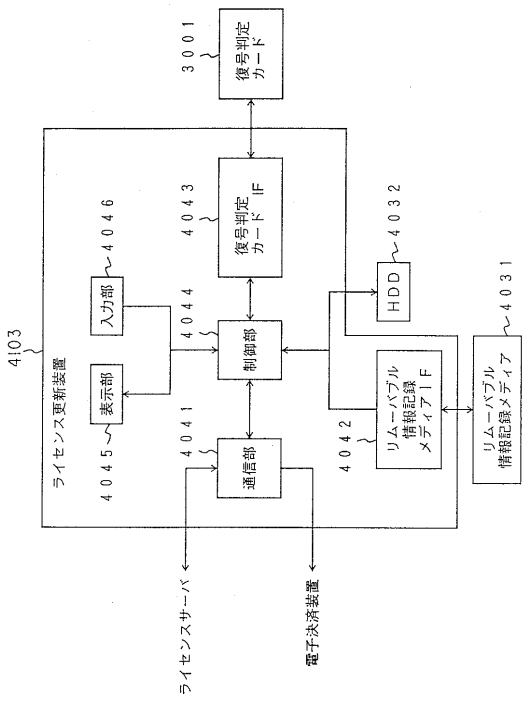
【図１０２】



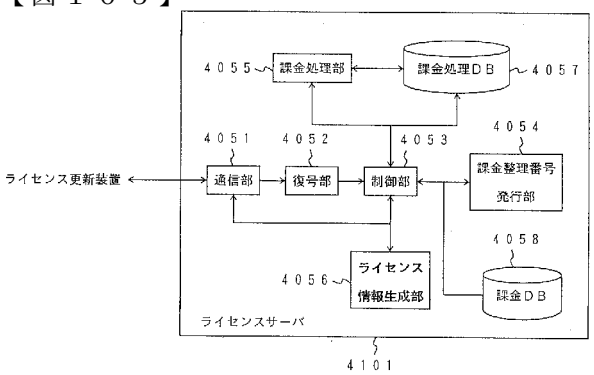
【図１０３】



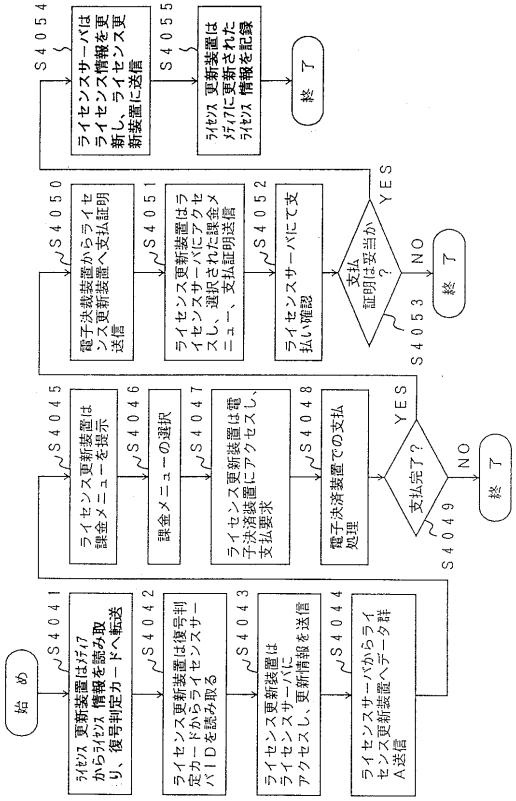
【図１０４】



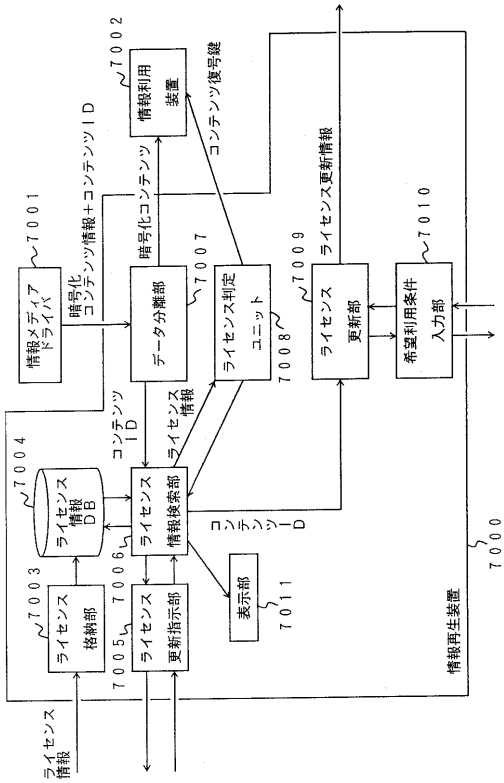
【図１０５】



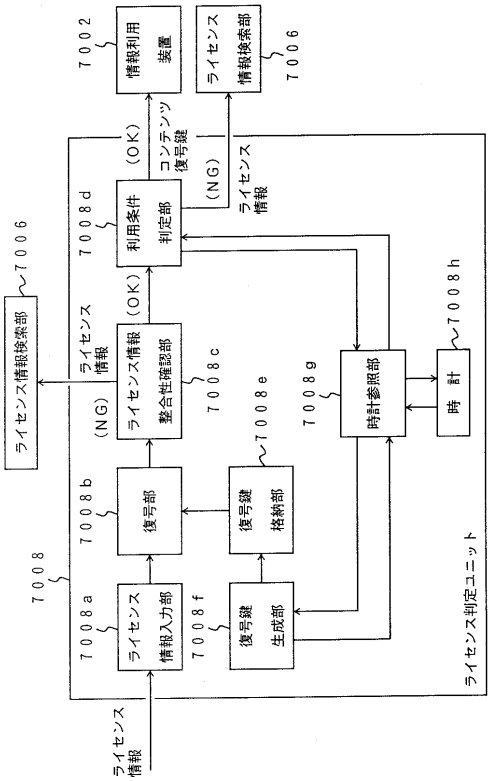
【図１０６】



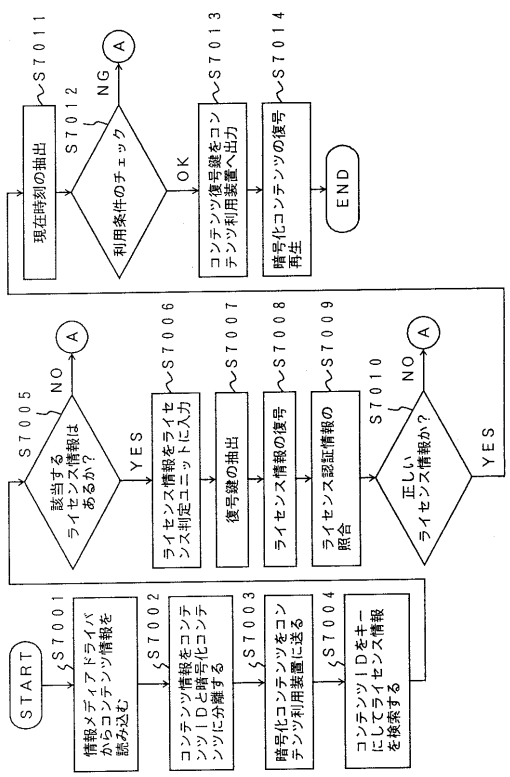
【図１０７】



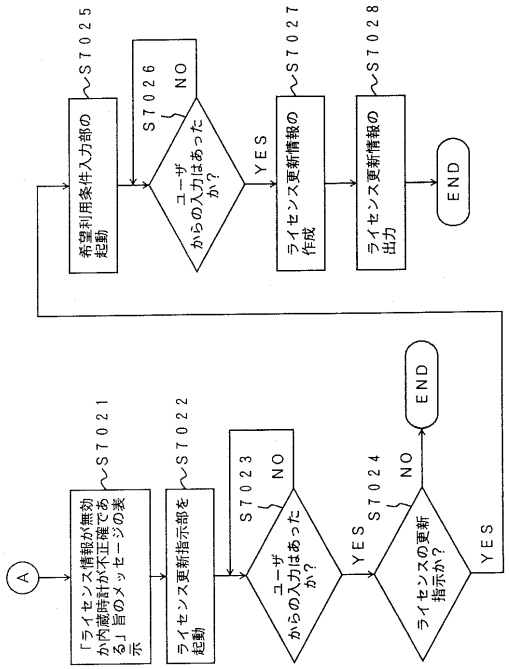
【図１０８】



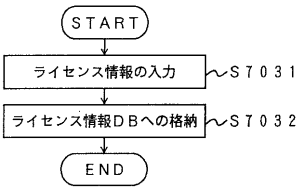
【図１０９】



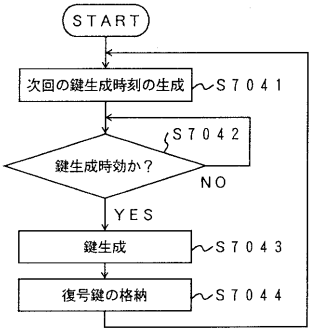
【図１１０】



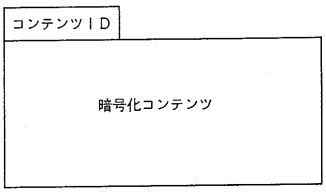
【図１１１】



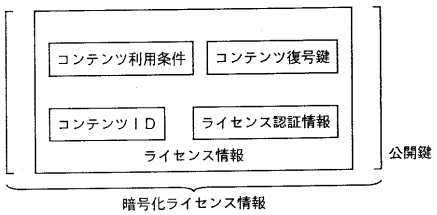
【図１１２】



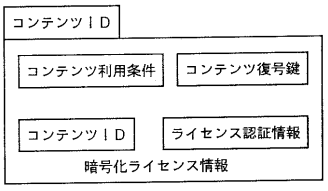
【図１１３】



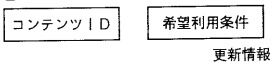
【図１１４】



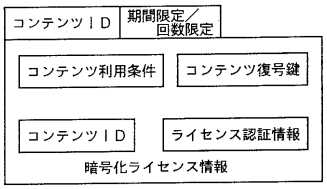
【図１１５】



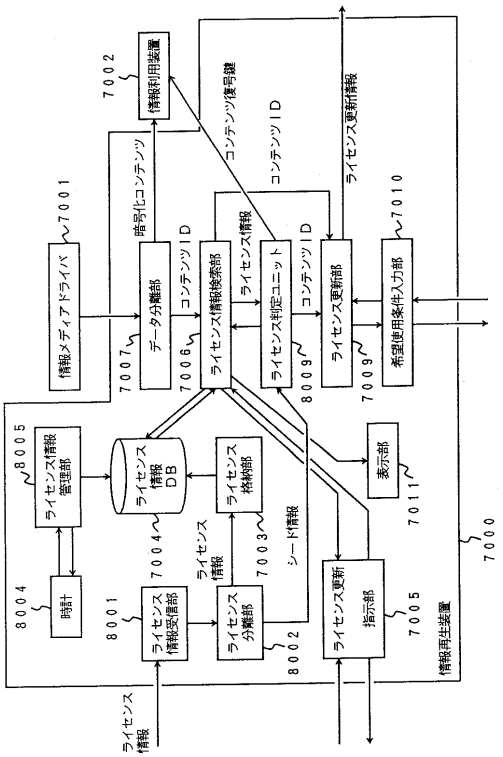
【図１１６】



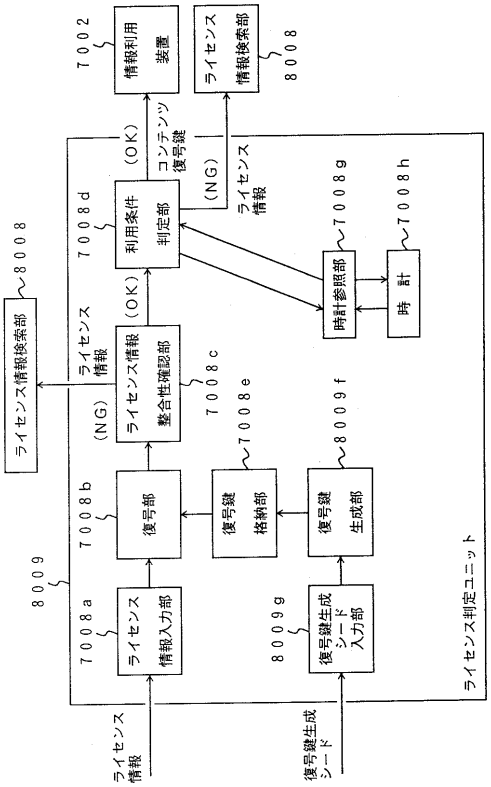
【図１１７】



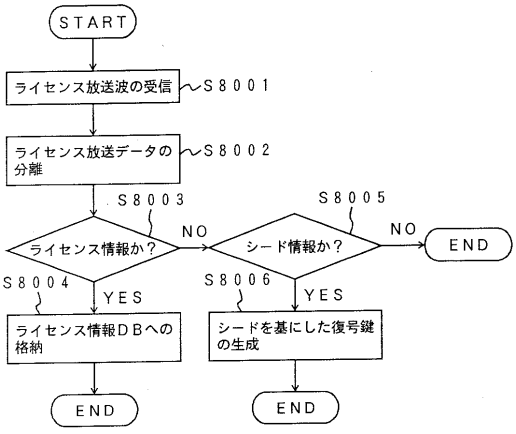
【図１１８】



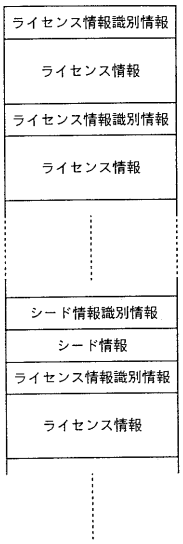
【図１１９】



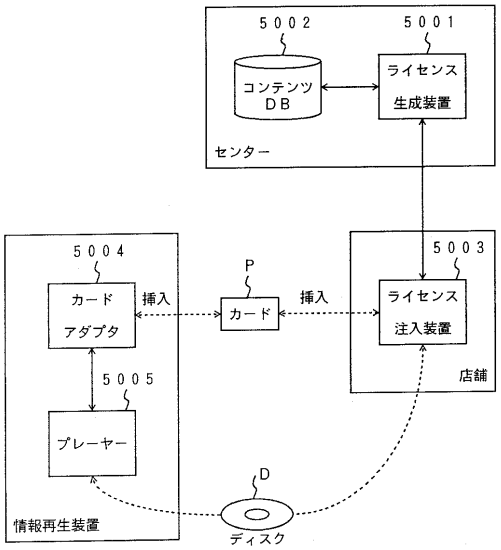
【図１２０】



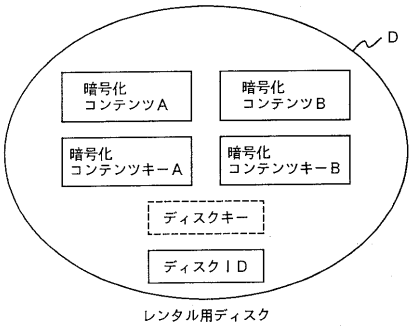
【図１２１】



【図１２２】



【図１２３】

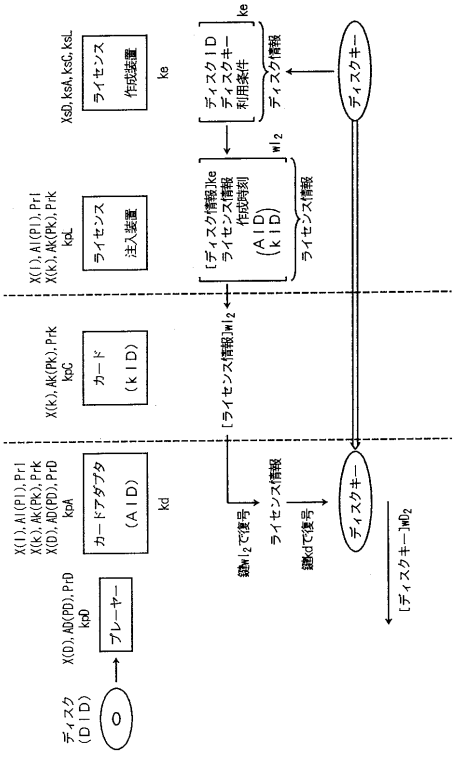


【図１２４】

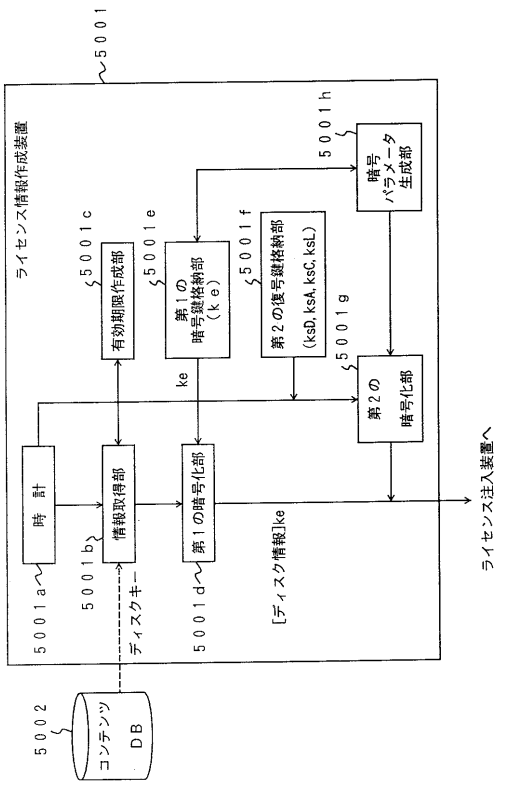
ディスクＩＤ	ディスクキー
０００１０２ ０００１０３ ……	１７６８ａｆｄｄ５ ４６５ｅｆｆａａｂ８９ ……

コンテンツＤＢ

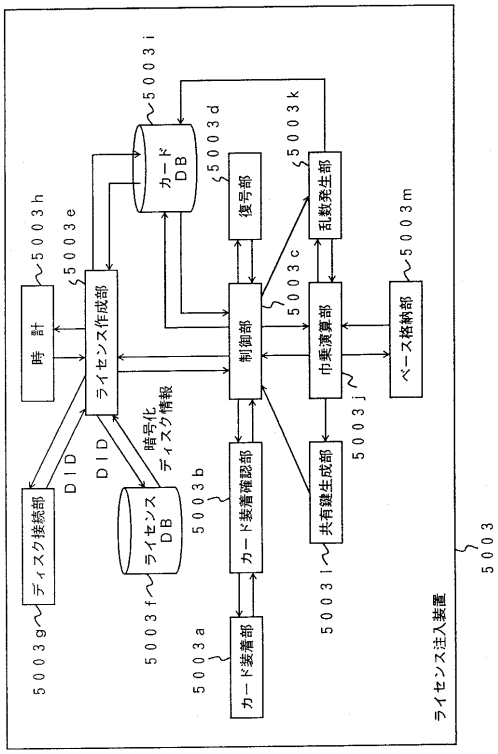
【図１２５】



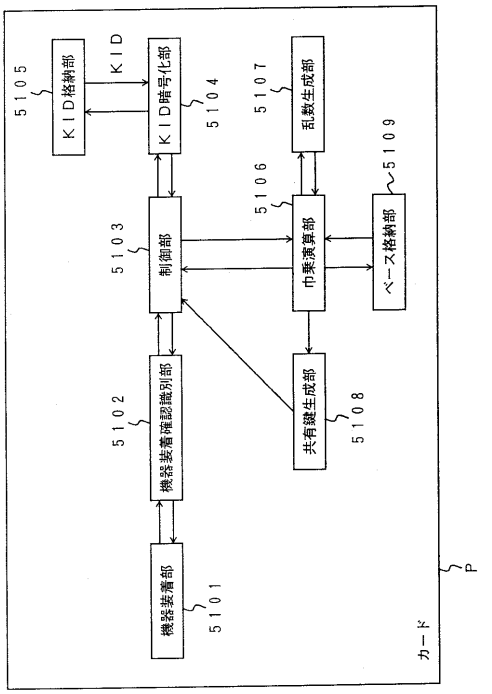
【図１２６】



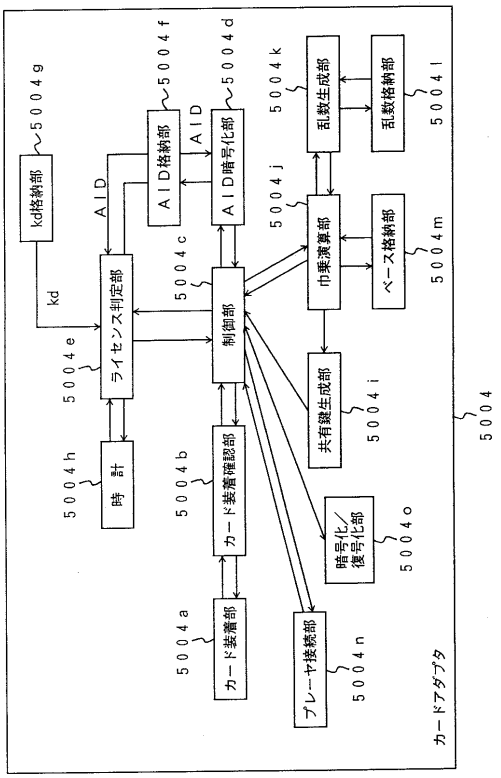
【図１２７】



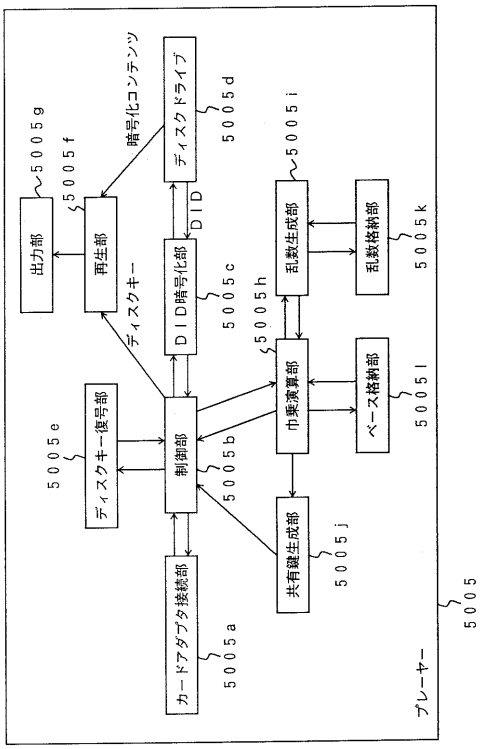
【図１２８】



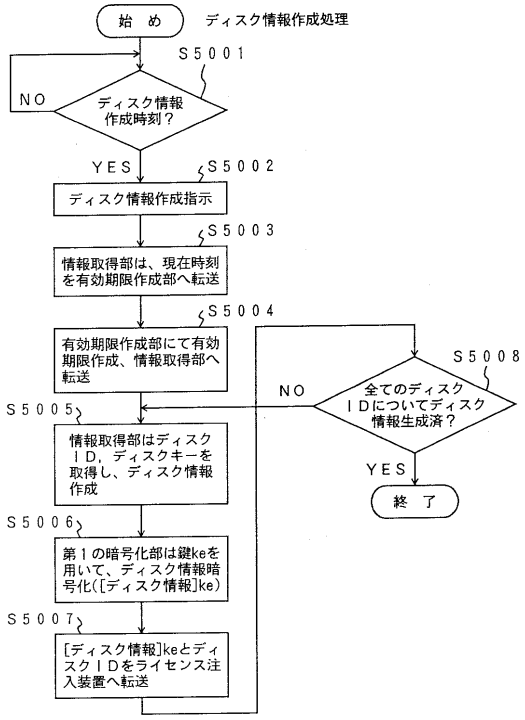
【図１２９】



【図１３０】



【図１３１】

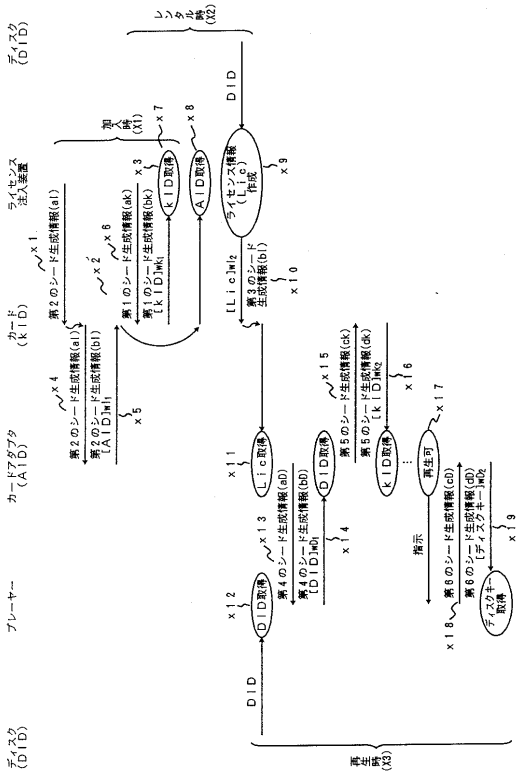


【図１３２】

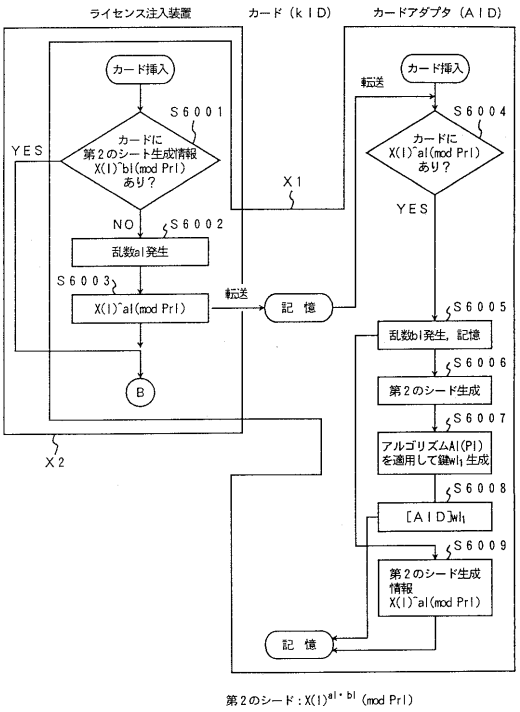
ディスクＩＤ	暗号化ディスク情報
0809eefd32	Fexx2039400x…
……	……

ライセンス注入装置　ライセンスＤＢ

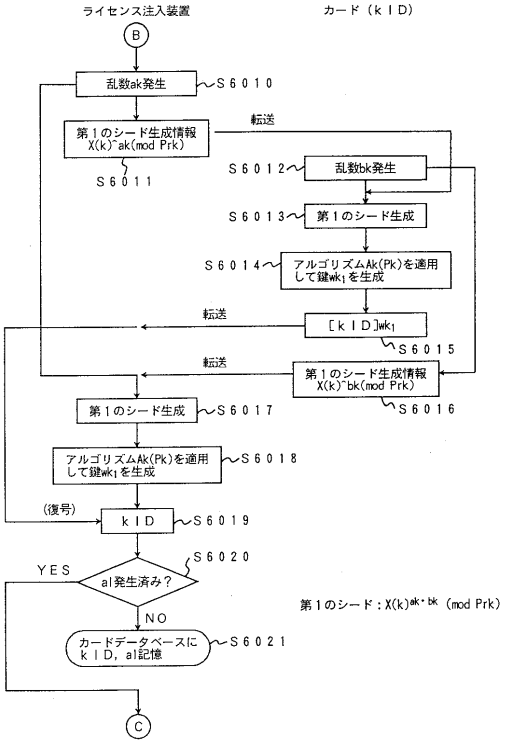
【図１３３】



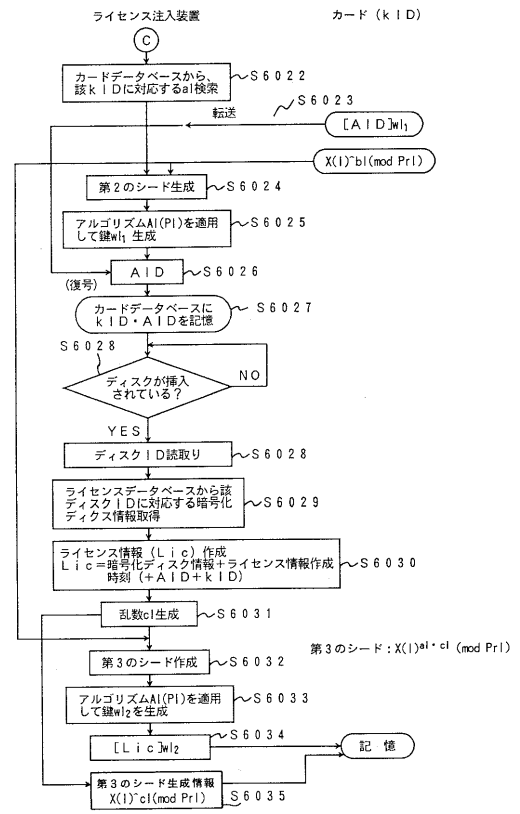
【図１３４】



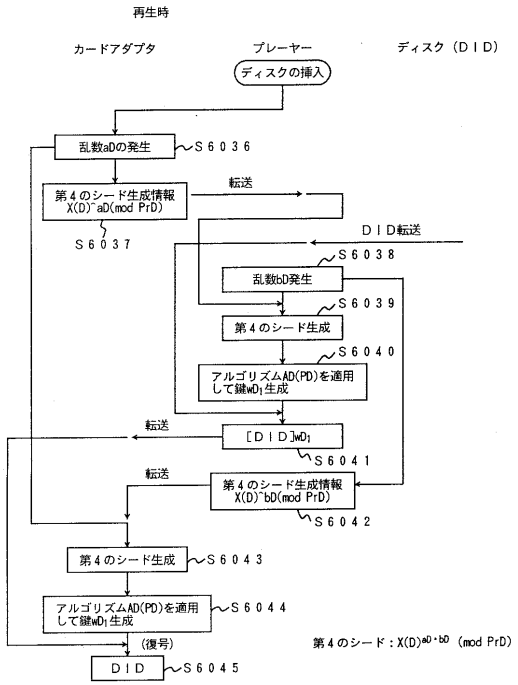
【図１３５】



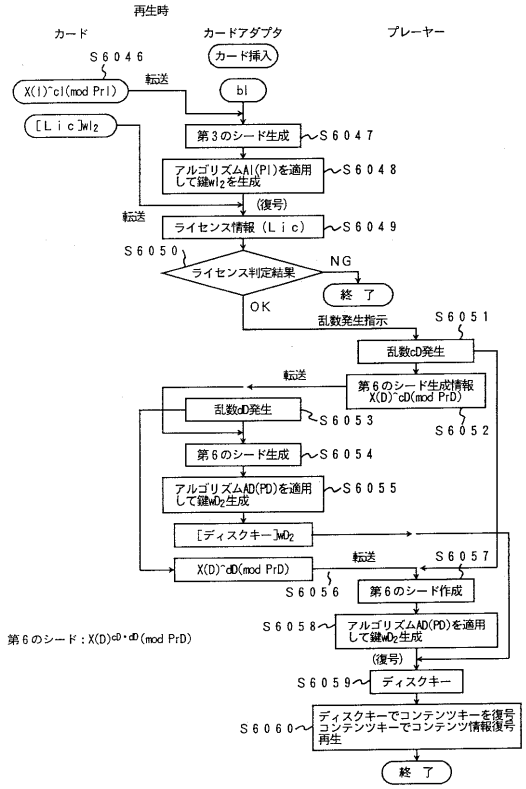
【図１３６】



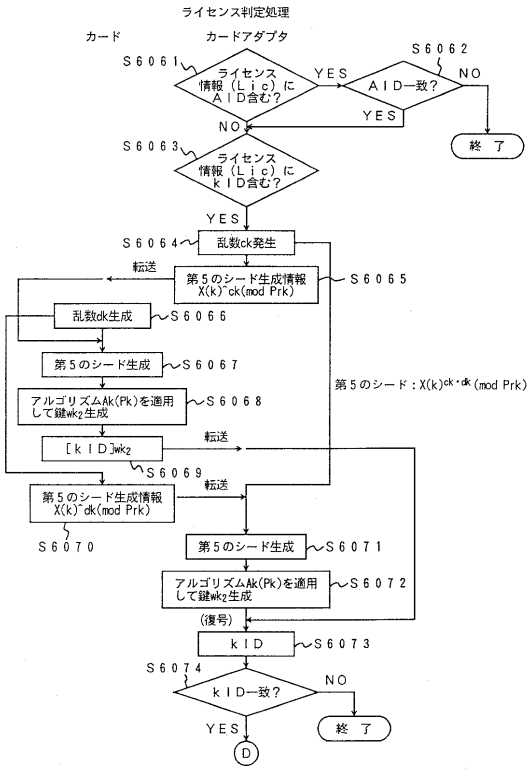
【図１３７】



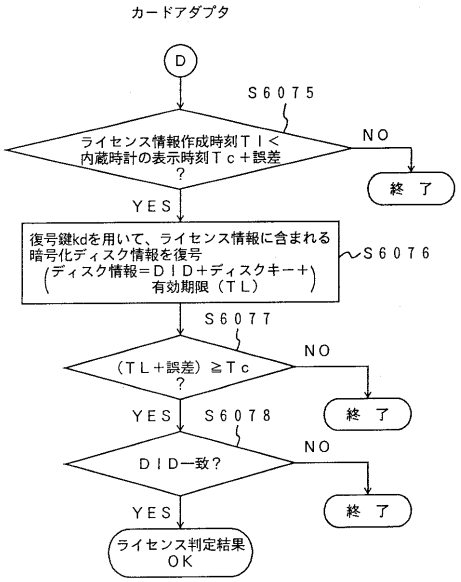
【図１３８】



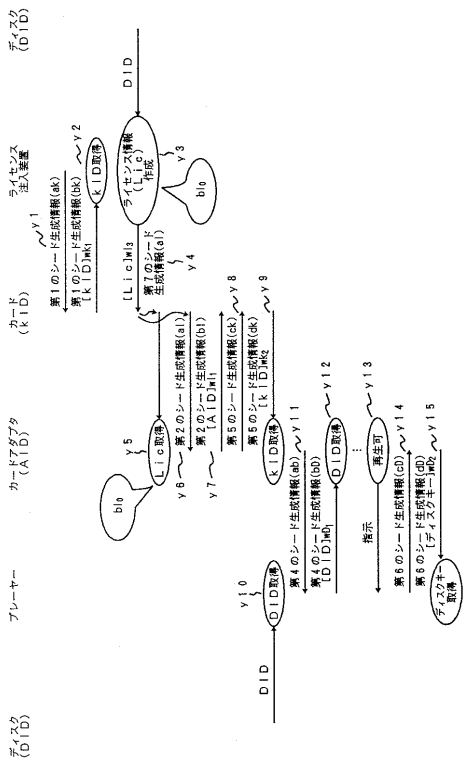
【図１３９】



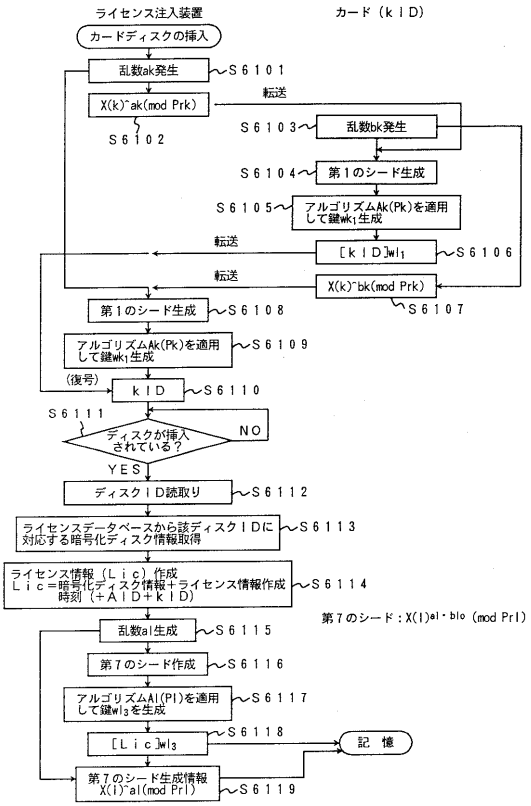
【図１４０】



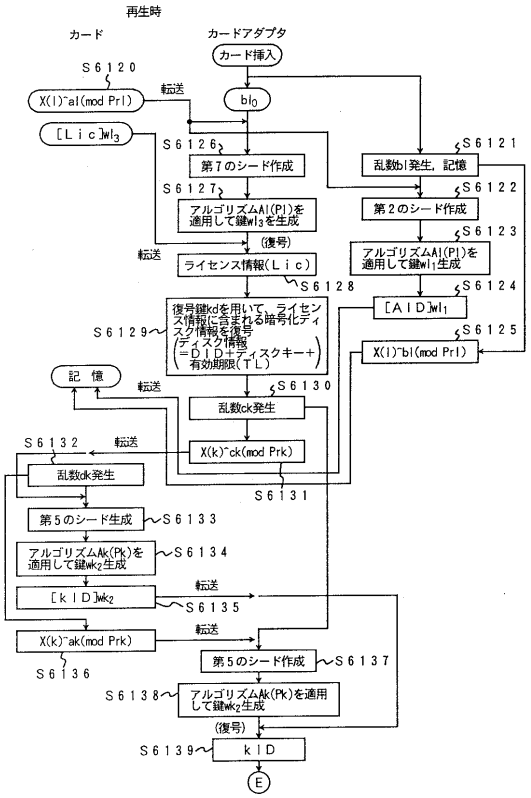
【図１４１】



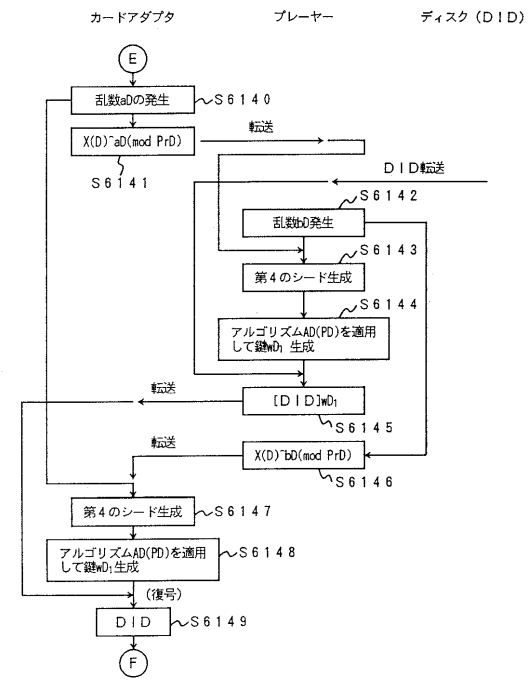
【図１４２】



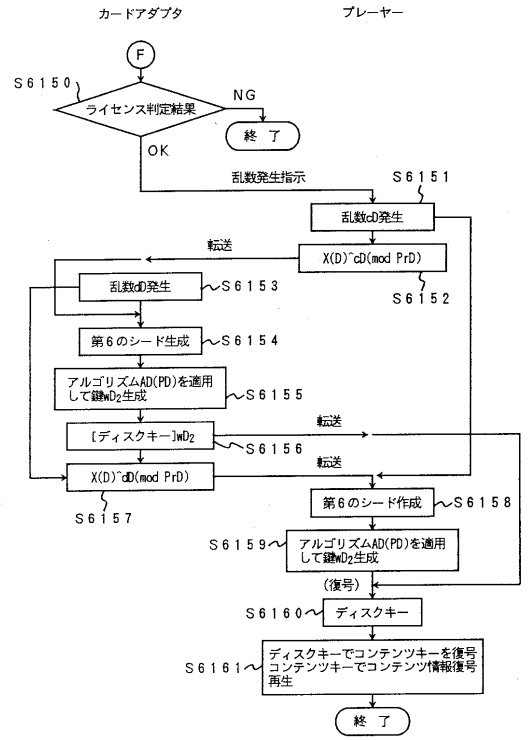
【図１４３】



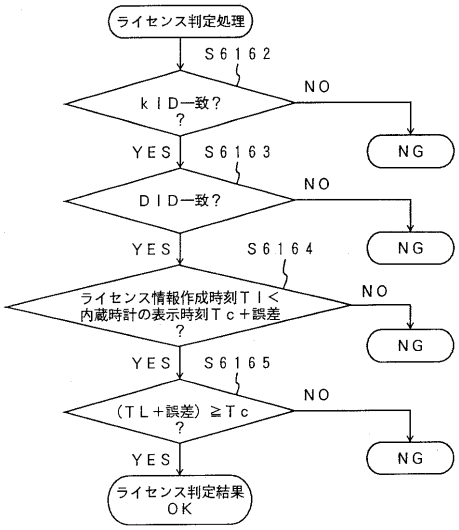
【図１４４】



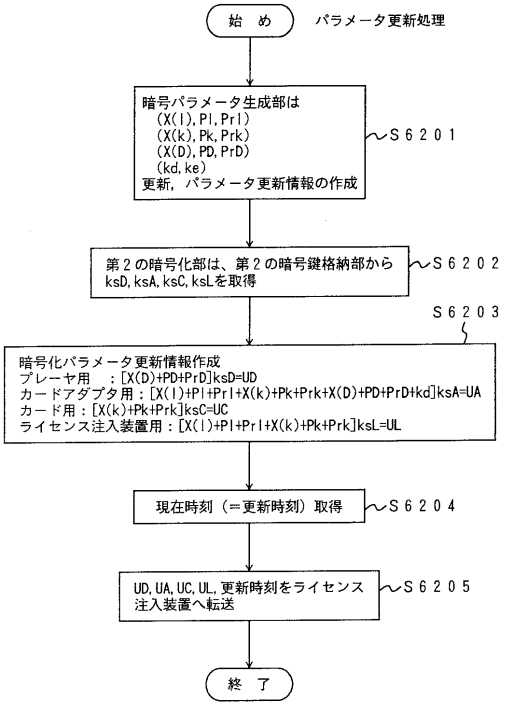
【図１４５】



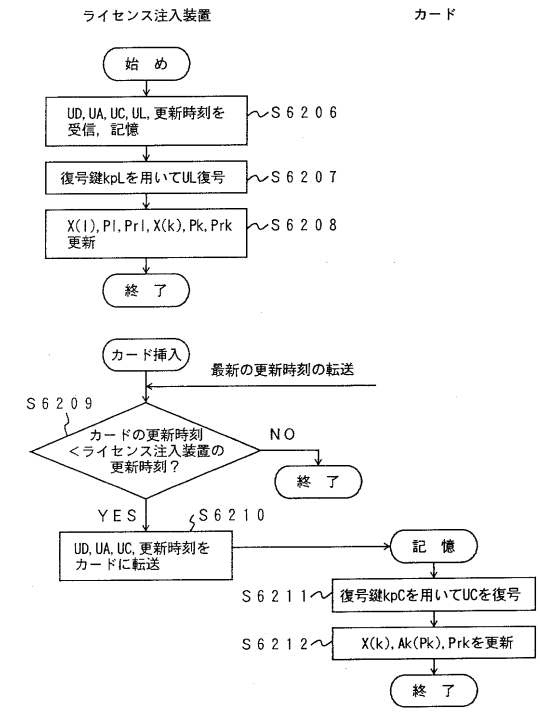
【図１４６】



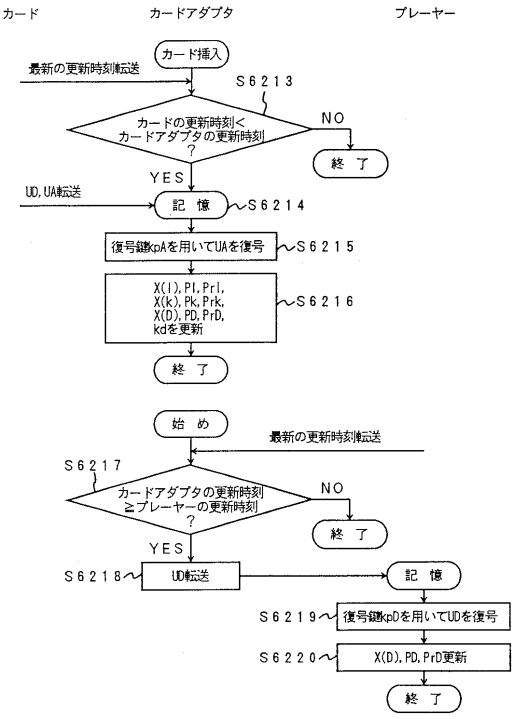
【図１４７】



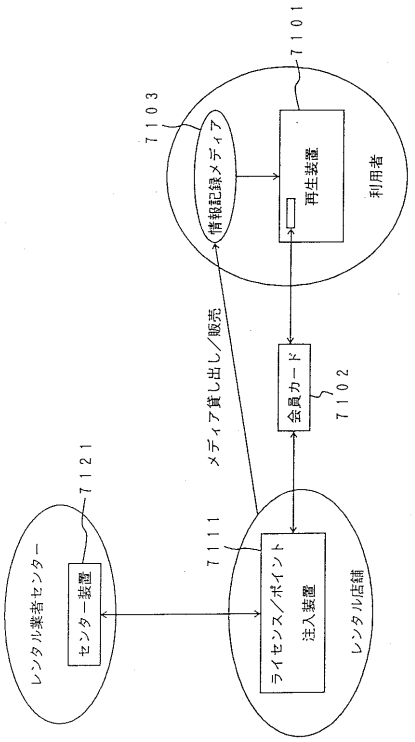
【図１４８】



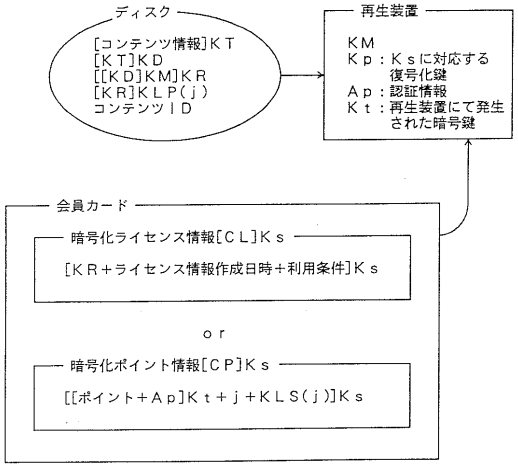
【図１４９】



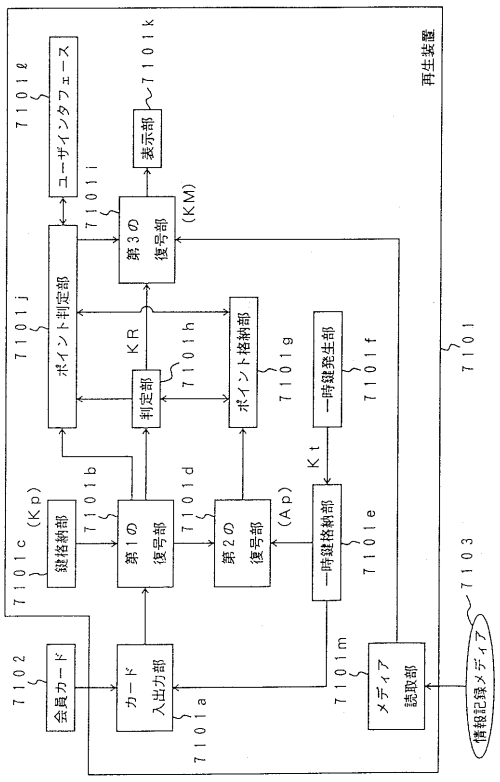
【図１５０】



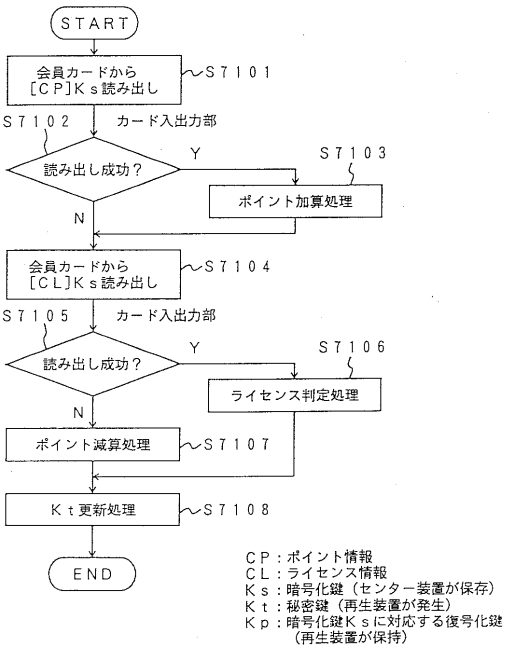
【図１５１】



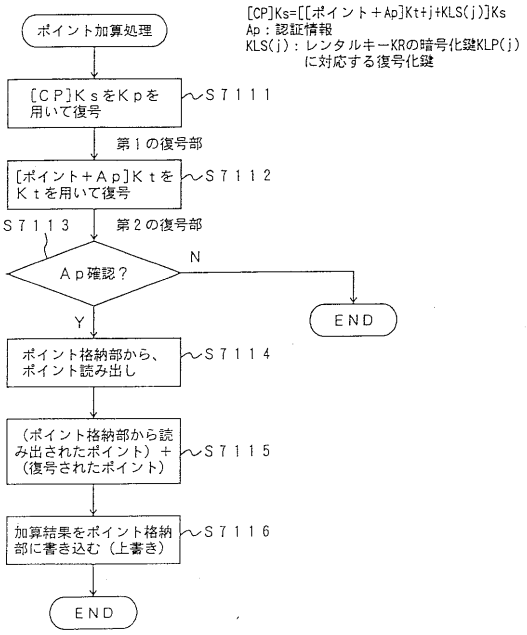
【図１５２】



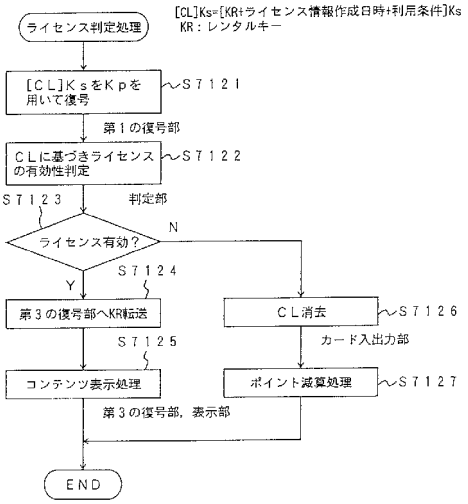
【図１５３】



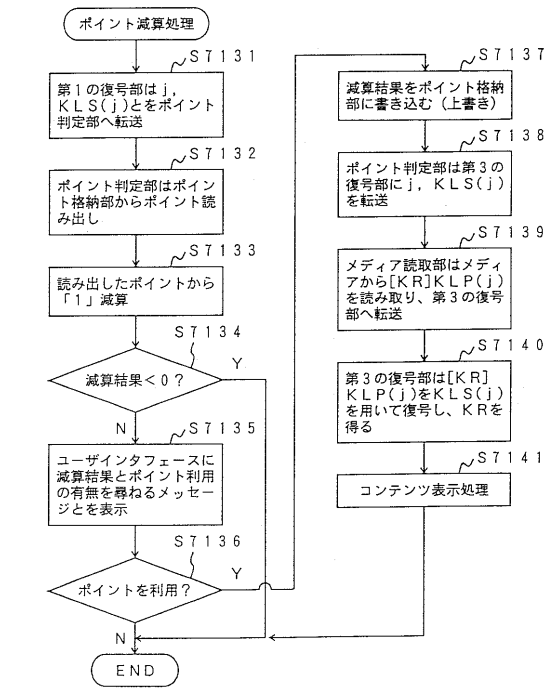
【図１５４】



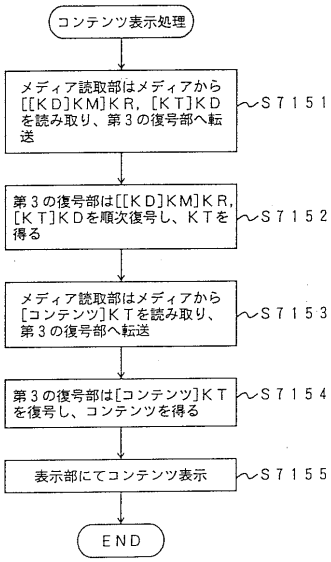
【図１５５】



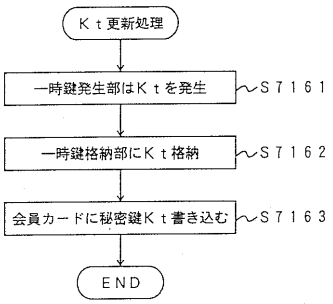
【図１５６】



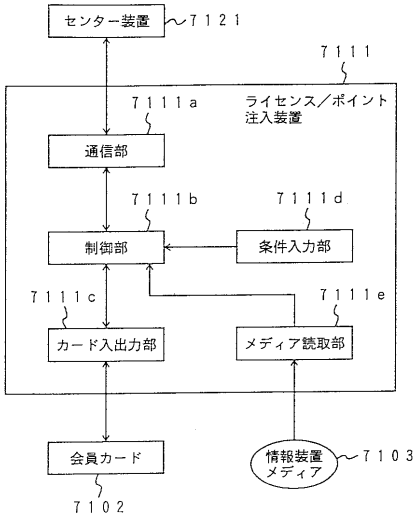
【図１５７】



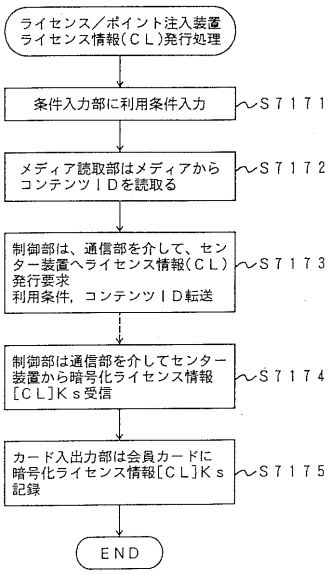
【図１５８】



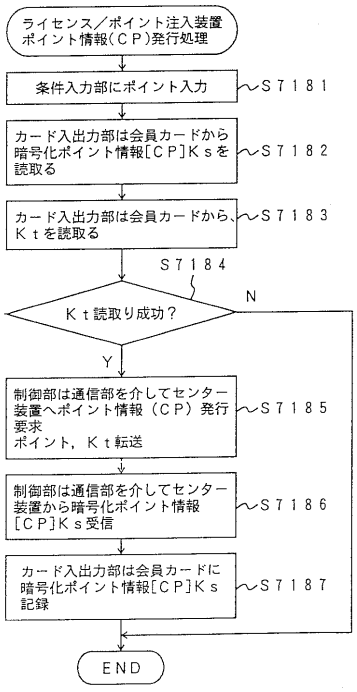
【図１５９】



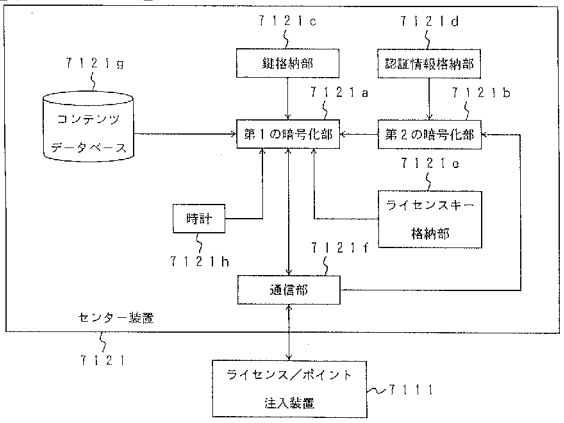
【図１６０】



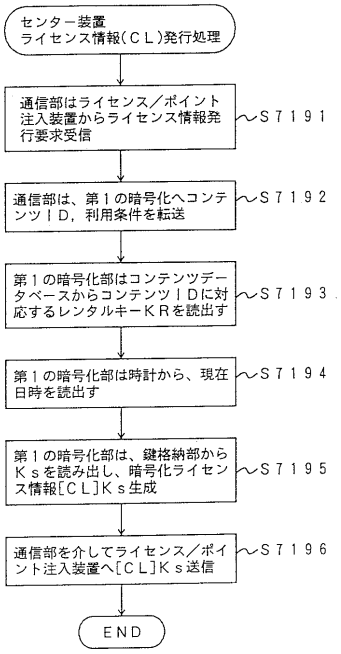
【図１６１】



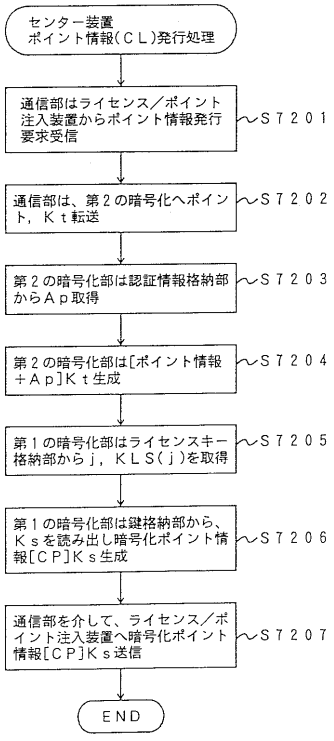
【図１６２】



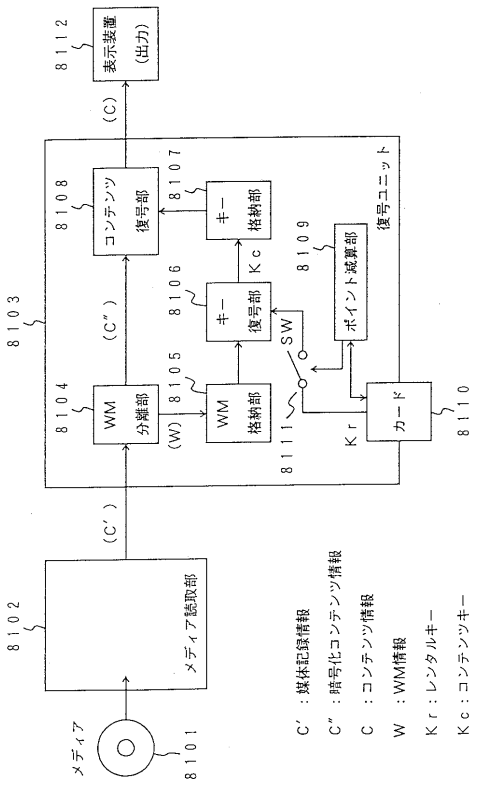
【図１６３】



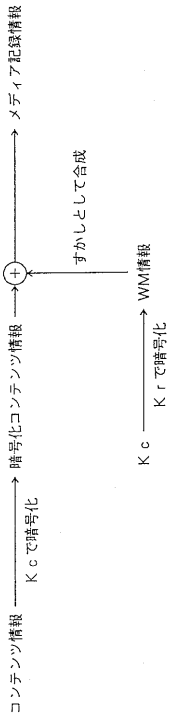
【図１６４】



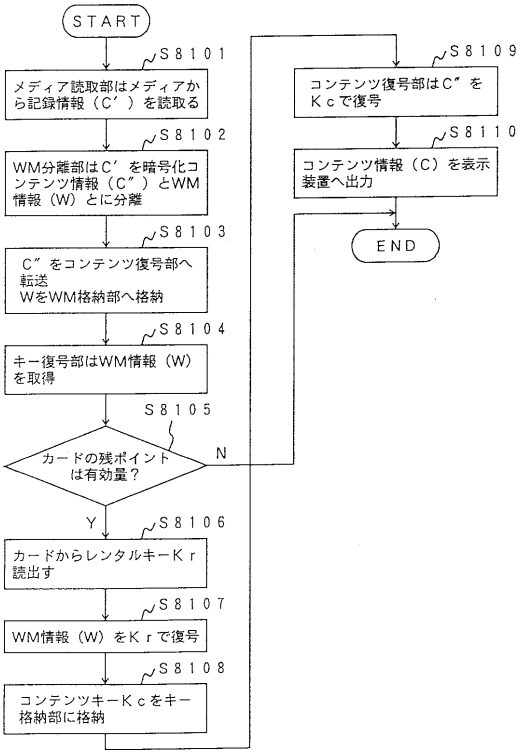
【図１６５】



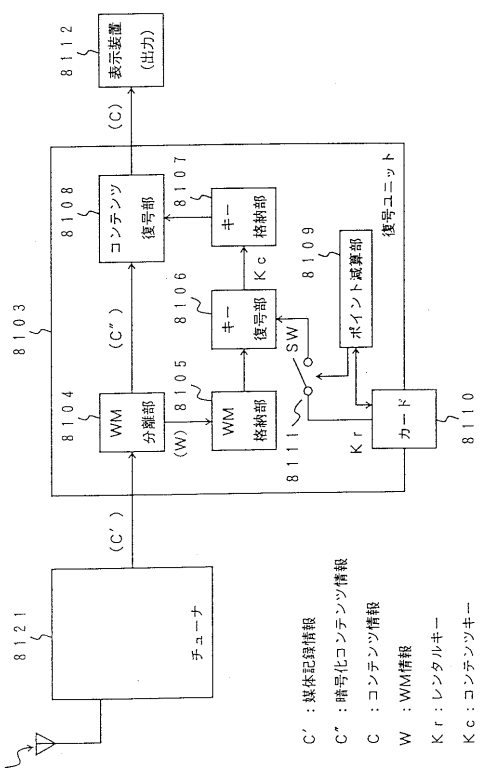
【図１６６】



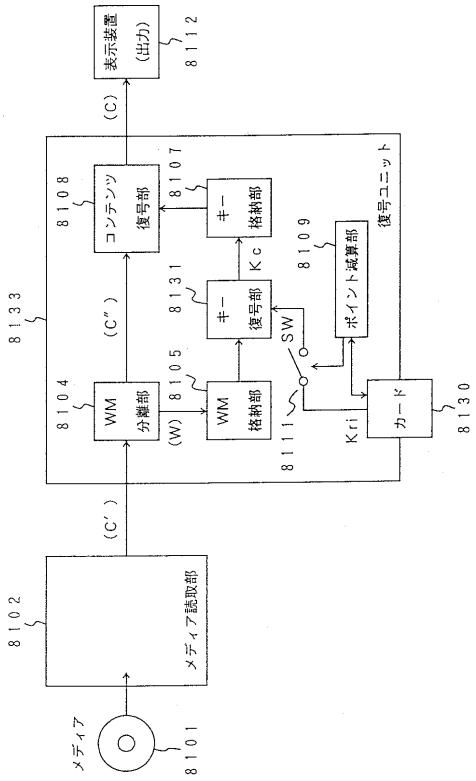
【図１６７】



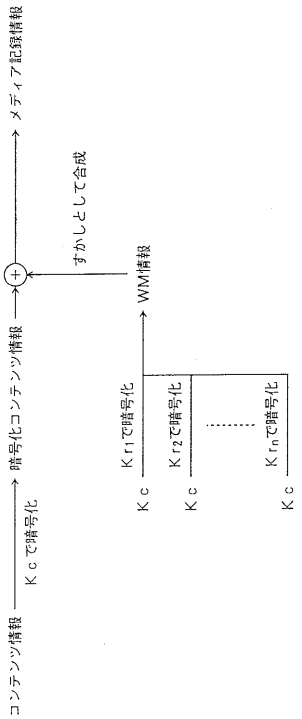
【図１６８】



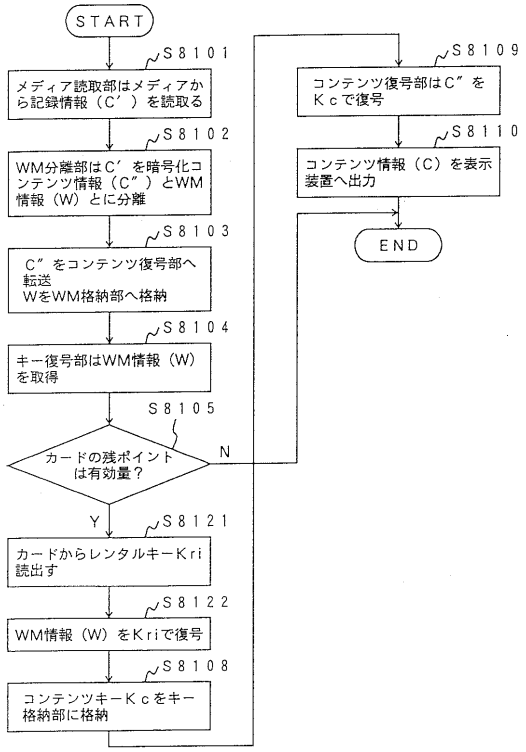
【図１６９】



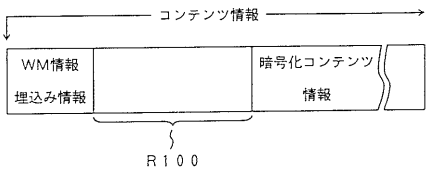
【図１７０】



【図１７１】



【図１７２】



フロントページの続き

(74)代理人 100070437
弁理士 河井 将次
(72)発明者 上林 達
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 秋山 浩一郎
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 辻本 修一
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 住田 一男
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 平川 秀樹
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 菅谷 寿鴻
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 梶浦 正浩
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内

審査官 平井 誠

(56)参考文献 特開平０７－２２１７５１（ＪＰ，Ａ）
特開平０７－１３１４５２（ＪＰ，Ａ）
特開平０９－１３８８２７（ＪＰ，Ａ）
森亮一，田代秀一，ソフトウェア・サービス・システム（ＳＳＳ）の提案，電子情報通信学会論文誌，日本，社団法人電子情報通信学会，１９８７年 1月２５日，Vol.J70-D No.1，ｐ．７０－８１，（引用非特許02-003103）
大瀧保広，超流通における暗号化の手法について，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，１９９１年 3月 8日，Vol90,No.460（ISEC90-44～53），33～42，（国内学会論文2000-00361-004）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24
G06F 21/22
G11B 20/10